Nortel Secure Networks

Entrust/Client

User Guide

for the Macintosh

Publication number: 68008.08
Date: January 1996
Software release: 2

Printed in Canada

This information is subject to change as Northern Telecom Limited reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances may warrant.

Contents

Using Entrust/Client 37

Hints 111

About this guide

Purpose of this user guide

This guide

- describes general cryptography concept
- details the Entrust/Client installation procedure
- gives step-by-step instructions on how to use Entrust/Client

What you need to know

This user guide is intended for people who have some experience using a Macintosh. Users should be familiar with terms like the following:

- desktop
- folders
- select and click

For information about these terms, refer to your Macintosh documentation.

You should also be familiar with the term *drag and drop*. If you are not, refer to “Dragging and dropping files” on page 26.

Terminology

The table below shows terms that are equivalent. The table also briefly describes the terms. The short terms are used most often to improve the readability of this document.

Term	Short version	Description
Entrust/Client	Client	a software application
Entrust/Client user	user	a person who uses the Client
Entrust Administrator	Administrator	the person who is responsible for maintaining all aspects of the Client
Certification Authority	CA	entity responsible for setting policies regarding the protection of sensitive and valuable data
CA security domain	domain	group of people who use Entrust under the same software license and have been certified by the same CA

The term *Entrust* used alone refers to Entrust products in general.

The expression *protected files* refers to files that have been encrypted, signed, or both encrypted and signed. Protected files have been processed by the Client in such a way that they can only be read by authorized people.

Notational conventions

The following types of information appear in italics:

- filenames
- titles of documents
- dialog names
- names of items that appear in dialogs
- terms that require emphasis

About Entrust/Client

Entrust/Client is an application that lets you encrypt and attach your digital signature to any file. You can also decrypt files and verify the signature of someone who sent you a file that was encrypted and signed using the Client.

The Client provides security features such as:

- data privacy
- signature authentication
- data integrity
- automated key management

Data privacy means only you and people you authorize (these people are called recipients) can view the contents of the files you encrypt.

Signature authentication means that you can check the digital signature of the person who signed a file. Data integrity means the file has not been altered since it was signed. The digital signature that accompanies a file is a guarantee that the file was signed by the author and that the file has not been altered since it was signed.

Automated key management means it is easy for you to encrypt and sign files for other people. The Entrust software keeps track of each Client user so you do not have to.

Table 1 on page 4 describes the main Entrust/Client features.

Table 1: Main Client features

Feature	Description
privacy	You have assurance that only you and authorized recipients can look at the contents of files you encrypt.
authentication	This feature allows you to verify the identity of the person who signed a file.
integrity	When you verify a signed file, this feature warns you if a file has been altered since it was signed.
portability	If you need to use Entrust/Client on a different computer than the one you normally use, you only need to transfer a copy of a file called your Client profile to the computer you want to use (provided the Client is installed on that computer). You can do this using a floppy diskette or any other file transfer mechanism. Your profile is portable across Macintosh computers, UNIX workstations, and PCs running Microsoft Windows.
address book services	This feature allows you to exchange protected files with a person who uses the Client in a different domain. For more information, see “Exchanging protected files with Entrust users in different domains” on page 71.
recipient lists	A recipient list is a set of options and recipients that you select and store under a recipient list name. Instead of having to specify each recipient and option every time you want to encrypt a file, you can specify the name of a recipient list. You control who is part of a recipient list and you can create more than one recipient list. For example, you could create one recipient list for each project you work on. For more information, see “Using saved lists of recipients” on page 80.

—continued—

Table 1: Main Client features (Continued)

Feature	Description
shared recipient lists	It is possible to share recipient lists with other Client users. Shared recipient lists let you maintain single copies of recipient lists and store them in a directory that is accessible to everyone who needs them. You can share your own recipient lists by exporting them. You can share other users' exported recipient lists by importing them.
ASCII file format support	This feature lets you encrypt files in a manner that ensures data integrity when you transfer files from one computer to another using a file transfer mechanism designed for ASCII transfer only.
file compression	You can compress protected files to save disk space. When compressed and protected files are received at the intended destination, they are automatically decompressed.
file archiving	You can use the *Archive* option to store multiple protected files in a single archive file. This is useful if you want to transfer several protected files; by storing all the protected files in a single archive file, you only need to transfer a single file. When the file is received at the intended destination and decrypted, the files are restored with their original filenames.
search bases	Your Security Officer can provide you with one or more search bases that you can use to reduce the scope of your recipient searches and thereby speed up the process of selecting recipients.
drag and drop	If you select one or more files and drag them to Entrust, the Client allows you to automatically encrypt and digitally sign files. If you drag one or more encrypted and/or signed files to Entrust, the Client automatically allows you to decrypt the files and verify the digital signatures associated with those files.

Reasons for using Entrust/Client

Protecting your work

Anyone who has access to your files, whether they are stored on floppy diskettes, hard disks, or a shared file server, can also see the contents of the files. In general, you may not mind if your colleagues can see the contents of your files; however, you probably have files that are sensitive and should only be seen by you and other people with whom you choose to share them. You can protect your sensitive files by using the Client to encrypt and sign them.

An encrypted file is completely unreadable. That means no one, including you, can read an encrypted file until it is decrypted. To decrypt an encrypted file is to restore it to its original state. Only you and other authorized recipients can decrypt the protected file and only you can determine who those recipients will be.

ATTENTION

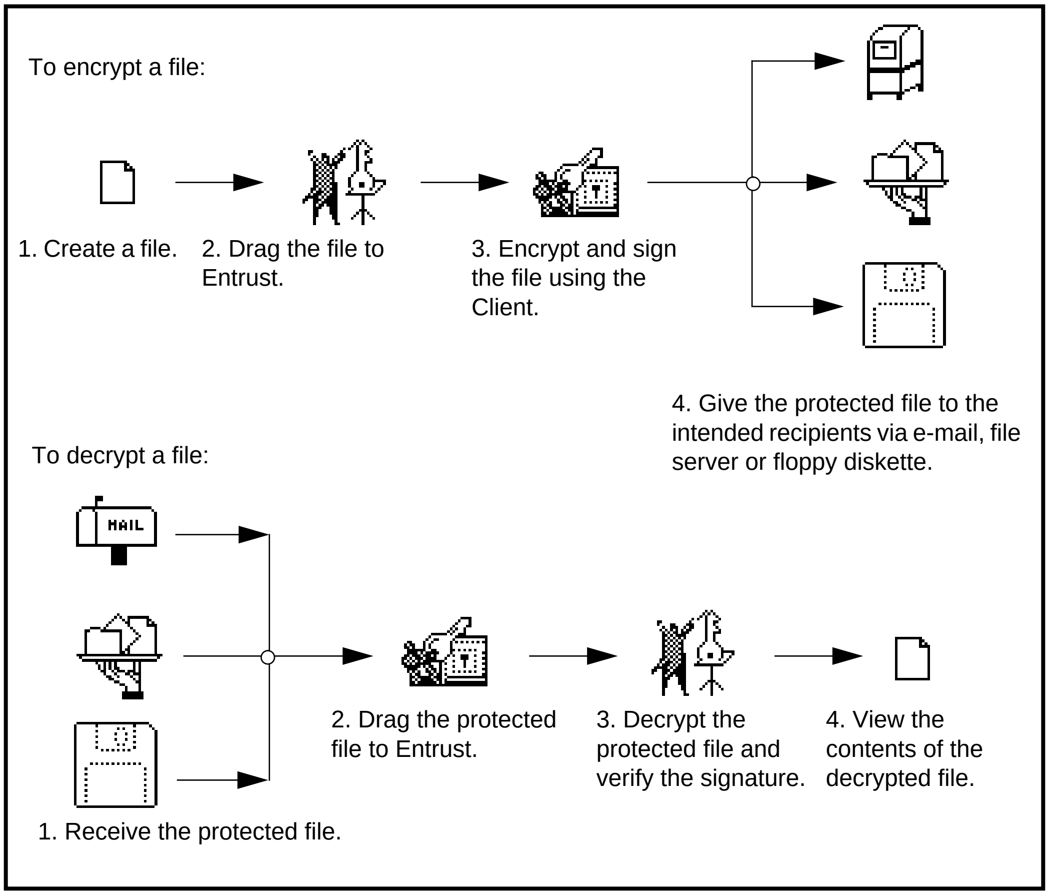
Entrust/Client does not prevent anyone from getting copies of your files. The Client makes it almost impossible for unauthorized people to view their contents.

Once the file is protected, you can give a copy to your intended recipients to decrypt and read when convenient.

There are no restrictions on how you combine recipients and encrypted files. For example, you can encrypt files for one group of people and then encrypt some other files for other groups or individuals. The Client keeps track of who is authorized to decrypt each individual file.

Entrust/Client is part of a suite of tools you use in your day-to-day activities. Note that using the Client is optional and is only necessary when you want to encrypt and sign a file. Figure 1 on page 7 summarizes the encryption and signing process, and the decryption and verification process.

Figure 1 Where Entrust/Client fits in your day-to-day activities


To encrypt a file:
1. Create a file.
2. Drag the file to Entrust.
3. Encrypt and sign the file using the Client.
4. Give the protected file to the intended recipients via e-mail, file server or floppy diskette.
To decrypt a file:
MAIL
1. Receive the protected file.
2. Drag the protected file to Entrust.
3. Decrypt the protected file and verify the signature.
4. View the contents of the decrypted file.

Since the file can only be decrypted by you and the recipients, it does not matter how you give the file to the recipients. You can put the file on a floppy diskette or in a shared folder on a file server, transfer the file using any electronic file transfer tool, or you can attach the protected file to an electronic mail message which you send to the recipients.

> ***Note:*** Protected files are in binary format. If you send protected files using an electronic file transfer tool, or as e-mail attachments, ensure these tools can handle binary files. If not, you can use the *ASCII encode after encryption* option when you protect files that are to be sent using tools that only handle ASCII files.

Signing documents electronically

You can use Entrust/Client to place your personal digital signature on a file whether or not you encrypt the file. This signature is a guarantee that the file came from you and that it has not been altered since you signed it.

A digital signature offers a certain level of protection even if a file is not encrypted because it is a guarantee that no one has tampered with the file. When a file is signed, you can use the Client to verify the signature. If the signature is valid, it means that the file has not been tampered with since the time it was signed. But if the signature verification fails, it means that the file may have been tampered with and that you should ask the person who gave you the signed file to sign it again and give you a new copy.

Sample uses of Entrust/Client

The following scenarios give examples of how people often use the Client in their day-to-day activities. Two fictional characters, named Bob and Alice, are used to describe the scenarios.

Encrypting a contract bid for a customer

Bob finally finished the sensitive contract bid he has been working on day and night for two weeks, and he needs to send it to his customer, Alice. Bob planned to use the mail to send the bid stored on a floppy diskette, but he worried that the diskette might fall into the wrong hands. Bob's bid must be protected from being read by anyone else. Since Alice also uses Entrust, Bob can easily protect his bid so that only she can retrieve the information. In addition, he can include his digital signature with the encrypted file to provide Alice with the added peace of mind that no one has tampered with his bid.

Before Bob sends the bid to Alice, he follows the procedure shown below.

1. Start the Client.
2. Specify the name of the recipient for this bid—in this case, Alice.
3. Encrypt and digitally sign a copy of the file containing the bid.
4. Copy the encrypted and signed file to a floppy diskette.

Now that Bob's bid is protected, he can simply put the floppy diskette in the mail, knowing that only Alice can read the contents. Even if the diskette falls into the wrong hands, he can be certain that its contents will not be revealed. Bob's file is protected by Entrust.

Encrypting employee yearly performance evaluations

Alice is preparing yearly performance review reports for her employees and wants to make the reports available to the other managers in her division. While Alice wants it to be easy for those managers to read the reports, she must ensure that the information remains confidential (employees must not have access to each other’s reports). The easiest way for Alice to make the reports available to the other managers is to store copies of the reports on a shared file server in her network. But since everyone in the company has access to this file server, she must ensure that only the managers can read the reports.

Before Alice stores copies of her employees’ yearly performance review reports on the file server, she follows the procedure shown below.

1. Start the Client.
2. Specify the names of the recipients for the reports—in this case, the other managers in Alice’s division.
3. Encrypt and digitally sign copies of each file containing an employee’s performance review.
4. Copy the encrypted and signed files to a directory on the file server.
5. Notify the managers that the files are available and that they must be unprotected before they can be read.

Encrypting an electronic mail message

Bob is working on a proposal for a new product that is likely to be a great commercial success, and he wants a colleague’s opinion on his work so far. The only problem is that Bob’s colleague, Alice, works in another city. Bob could fax a copy of his proposal, but he hesitates since it is critical that the proposal remain secret until it is ready to be unveiled. Bob decides to send the proposal to Alice as an attachment to an electronic message.

In general, sending a file attached to an electronic mail message makes the contents of the file accessible to anyone who can read copies of other people’s electronic mail as it is transmitted over the network. The technology for this type of illegal activity is readily available.

Because of the highly sensitive nature of the proposal and the great potential for disaster if it were to fall into the wrong hands, Bob decides to protect it from being read by anyone else. Since Alice also uses Entrust, he can use the Client to protect the proposal.

To protect a copy of the proposal before sending it, Bob follows the procedure shown below.

1. Start the Client.

2. Specify the name of the recipient for the proposal—in this case, Alice.
3. Encrypt and digitally sign a copy of the file containing the proposal.
4. Switch to an electronic mail tool.
5. Compose an electronic mail message to Alice (in this case) asking for opinions on the proposal.
6. Attach the encrypted and signed proposal to the mail message.

Bob can now safely send the proposal.

Alice detaches the file containing the proposal, decrypts it, annotates the proposal with comments, re-encrypts it, and returns it to Bob using electronic mail.

No one except Bob and Alice can ever know the contents of the proposal until Bob decides to make the information available.

Signing a form

In an effort to move towards a paperless office, Alice’s company has online versions of its business forms (for example, expense reports). Alice routinely completes such forms directly online using her computer. Then she has to print the form for her supervisor Bob to sign.

Instead of printing the form for signature, Alice can use the Client to digitally sign the form and send it electronically to Bob for authorization. Bob checks the form, authorizes it by digitally signing it (without printing it to paper), and sends it directly to Accounting. Because the form does not contain sensitive information, it does not need to be encrypted.

Since Accounting also uses Entrust, the signature on the form can be verified to ensure that the form was authorized by Bob and that it has not been altered by anyone.

Alice would first follow the procedure shown below.

1. Open the file containing the form and fill it out online.
2. Save the changes in a file.
3. Use the Client to sign the file.
4. Use the file transfer mechanism of choice to send the file to Bob.

Bob would then follow the procedure shown below.

1. Start the Client.
2. Verify the form.
3. Use the Client to sign the file.

4. Use a file transfer mechanism to forward the file to Accounting.

Accounting would then follow the procedure shown below.

1. Start the Client.
2. Use the Client to verify Bob's signature and the integrity of the contents of the file.

What Entrust/Client is not

The Client is neither a substitute for your existing electronic mail software nor is it a substitute for an electronic file transfer mechanism. Once you have protected a file using the Client, you must use an existing tool to give the protected file to your recipient. An Entrust recipient should not be considered equivalent to an electronic mail recipient.

Before you begin

Before you begin to install and use Entrust/Client:

- Ensure the computer you plan to use with the Client meets the minimum requirements specified in “Minimum system requirements” on this page.
- Obtain your start-up package from your Administrator (refer to “Start-up package” on page 14).
- Read “Important information about passwords” on page 15.

Minimum system requirements

The following are the minimum hardware and software requirements for running the Client:

- 4 megabytes of RAM
- 1 double-sided high-density (1.44 megabyte) diskette drive (only if you plan to install from a floppy diskette)
- System 7.0 or better

Start-up package

Before you can install and use the Client, you need to obtain important information and files from your Entrust Administrator. Ask your Administrator to give you the following information:

- an Entrust user reference number
- an Entrust user authorization code
- access to the installation software

Reference number and authorization code

You need a reference number (for example, 22172260) and an authorization code (for example, 7GNP-QI36-HAWG) to create your Client username. The reference number and authorization code can only be used once. If there is a need to create more than one Client username on a single computer (for example, because two people share one computer and both need to use Entrust), refer to "Creating additional Entrust/Client users" on page 93.

Your Administrator will tell you your reference number and authorization code in a confidential and secure manner.

ATTENTION

Keep your reference number and authorization code confidential. Ensure you destroy them after you have created your Client username.

Installation software

You will need the software required to install the Client. Your Administrator will either give you the software on diskettes or put it in a shared folder on a server.

Important information about passwords

Your Entrust/Client password is a critical link in the security chain. You should never reveal your password to anyone. You should guard your password just as you would a banking card personal identification number (PIN) or other valuable information.

ATTENTION

If you write down your password, ensure it is stored in a locked place that only you can access. Anyone with access to your password and your Client profile will have the ability to view your protected files and sign files with your signature. If you forget your password or if you suspect that someone has obtained your password, contact your Entrust Administrator.

It is important that you select passwords that are difficult to guess or derive. Avoid using the following as passwords because they are easy for an intruder to obtain:

- common or proper nouns
- birth dates
- employee numbers
- social security numbers
- any number that can be associated with you

When you choose a password, invent a word and include special characters for good measure. Examples of special characters are: $, +, !, =, ~, ^ and &. A good password is one that is difficult to guess and easy to remember (for example, H2OPlsNow! (water please, now!)).

In addition, the software enforces certain rules. Your password must

- be at least eight characters long
- contain at least one upper case letter
- contain at least one lower case letter
- not contain many occurrences of the same character
- not be the same as your Entrust/Client username
- not contain a lengthy substring of your Entrust/Client username

For more information about password criteria and how Entrust manages password security, refer to “Appendix C: Entrust password security.”

Getting help

If you need help, contact your Entrust Administrator.

Quick start to using Entrust/Client

This chapter gives you the basic information you need to start using the Client. It provides you with step-by-step instructions for completing the following tasks:

- installing the Client
- starting the Client
- creating a Client username
- encrypting and signing a file
- decrypting and verifying an encrypted and signed file
- ending your Client session

Installing the Entrust/Client

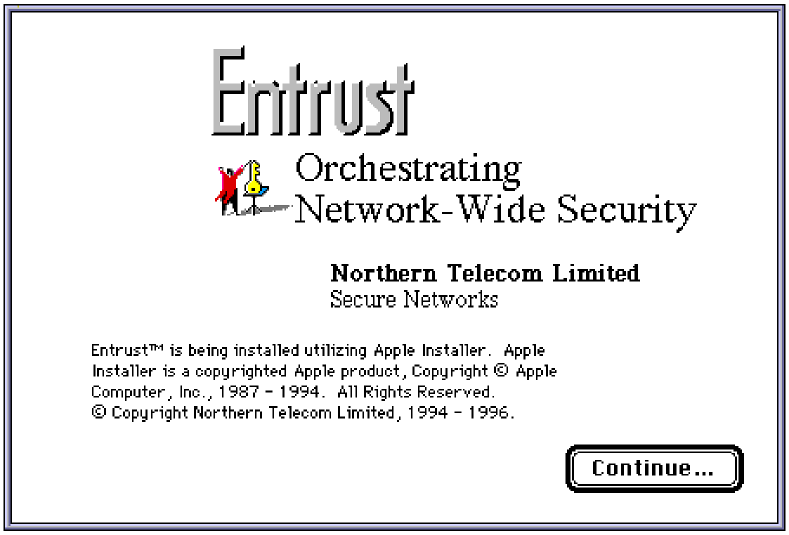
Before you install the Client, quit all applications that are currently running.

1. Access the installation software.

This software is either stored in a shared volume on a file server, or on floppy diskettes. Your Administrator will tell you where the installation software is stored.

2. Double-click the *Entrust Installer Script* file.

The installation software starts up and the following dialog appears.



Entrust

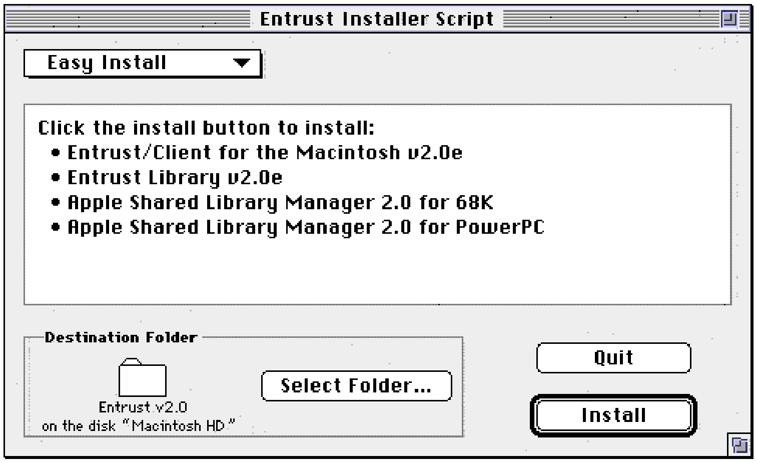
Orchestrating Network-Wide Security

Northern Telecom Limited
Secure Networks

Entrust™ is being installed utilizing Apple Installer. Apple Installer is a copyrighted Apple product, Copyright © Apple Computer, Inc., 1987 - 1994. All Rights Reserved.
© Copyright Northern Telecom Limited, 1994 - 1996.

3. Click *Continue...*

The *Entrust Installer Script* dialog appears.



Entrust Installer Script

Easy Install

Click the install button to install:
- Entrust/Client for the Macintosh v2.0e
- Entrust Library v2.0e
- Apple Shared Library Manager 2.0 for 68K
- Apple Shared Library Manager 2.0 for PowerPC

Destination Folder

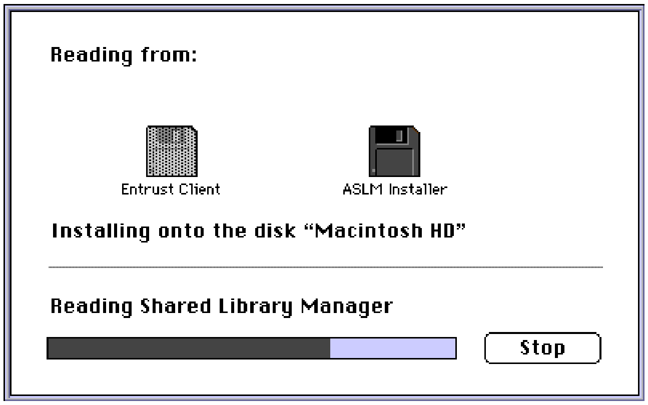
Entrust v2.0
on the disk "Macintosh HD"

4. Notice the *Destination Folder* area in the *Entrust Installer Script* dialog.

   It shows the name of the folder in which the Entrust/Client software will be installed. Ensure that the current folder is on your start-up disk; that is, the disk on which your *System Folder* is stored. Click *Select Folder...* to specify a different folder.

5. Click *Install*.

   The following dialog appears.

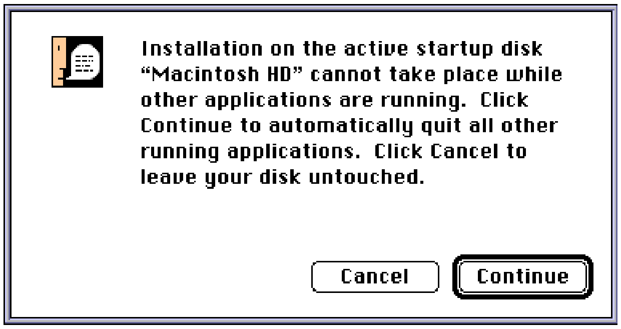


Reading from:

Installing onto the disk "Macintosh HD"

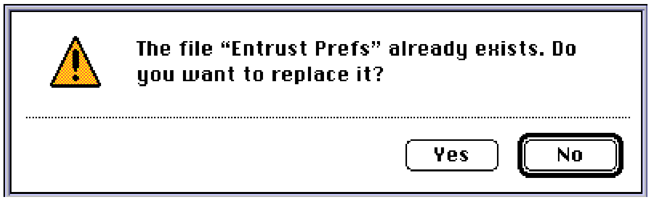
Reading Shared Library Manager

Note: If other applications are running at the same time, the following dialog appears. If this happens, click *Continue*. The installation software will give you the opportunity to save any open files before quitting the applications that are currently running.



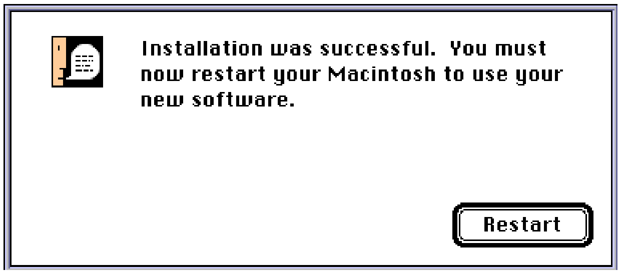
Installation on the active startup disk "Macintosh HD" cannot take place while other applications are running. Click Continue to automatically quit all other running applications. Click Cancel to leave your disk untouched.

Note: If you are upgrading from a previous version of Entrust/Client, the following dialog appears. Your *Entrust Prefs* file contains information specific to the Entrust installation in your domain. It is unlikely that you want to replace your existing *Entrust Prefs* file. Click *No* to retain your existing *Entrust Prefs* file. Your Entrust Administrator will tell you if you need to replace your *Entrust Prefs* file.



The file "Entrust Prefs" already exists. Do you want to replace it?

When the installation is complete, the following dialog appears.

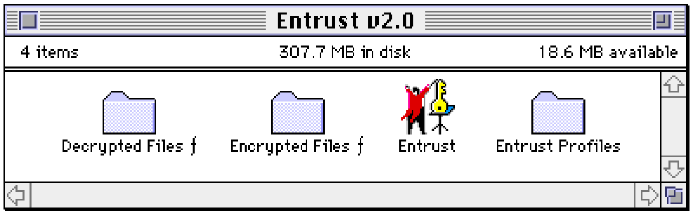


Installation was successful. You must now restart your Macintosh to use your new software.

6. Click *Restart.*

Your Macintosh is automatically restarted.

The Client is installed on your Macintosh. A folder containing the following icons appears in the folder in which you installed the Client. If you choose, you can use the *Encrypted Files ƒ* folder to store your protected files and the *Decrypted Files ƒ* folder to store your unprotected files.



Entrust v2.0

4 items 307.7 MB in disk 18.6 MB available

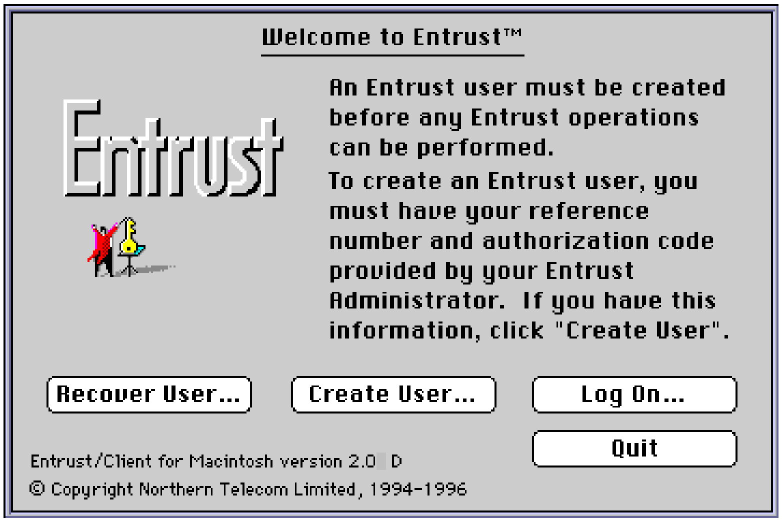
At this time, you can also make an alias of the *Entrust* icon using the *Make Alias* option under the *File* menu in the *Finder.* You can store the alias icon on your desktop for convenient drag-and-drop access to the Client.

Starting Entrust/Client for the first time

Once you have installed the Client, you can create a Client username and begin to use it. Proceed as follows.

1. Double-click the *Entrust* icon.

2. The *Welcome to Entrust* dialog appears.



Welcome to Entrust™

An Entrust user must be created before any Entrust operations can be performed.

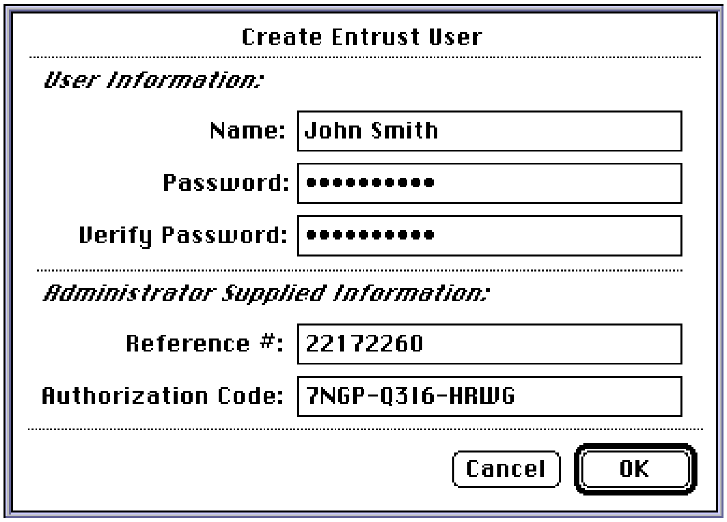
To create an Entrust user, you must have your reference number and authorization code provided by your Entrust Administrator. If you have this information, click "Create User".

Entrust/Client for Macintosh version 2.0 D

© Copyright Northern Telecom Limited, 1994-1996

3. Click *Create User...*

The *Create Entrust User* dialog appears.



Create Entrust User

User Information:

Name: John Smith

Password: ●●●●●●●●●●●

Verify Password: ●●●●●●●●●●●

Administrator Supplied Information:

Reference #: 22172260

Authorization Code: 7NGP-Q316-HRWG

4. Enter your name in the in the *Name* field.

   You may choose any name you like (for example, *John Smith*).

5. Tab to the *Password* field and enter a password.

   Your Client password must

   - be at least eight characters long
   - contain at least one upper case letter
   - contain at least one lower case letter
   - not contain many occurrences of the same character
   - not be the same as your Client username
   - not contain a substring of your Client username

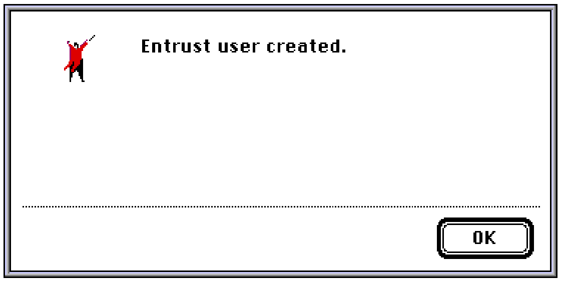
   The password is case-sensitive. When entering a password, avoid using a common or proper noun. Try to invent a word and include special characters for good measure. Examples of special characters are: $, +, =, !, ~, ^ and &. A good password is one that is difficult to guess and easy to remember (for example, H2OPlsNow! (water please, now!)). For more information about passwords, refer to “Appendix C: Entrust password security.”

6. Tab to the *Verify Password* field and enter the same password again.

The reason you need to enter your new password twice is to ensure that you typed exactly what you meant to type. Entrust checks to ensure that you entered your new password exactly the same way both times.

7. Tab to the *Reference #* field and enter the reference number you obtained from your Administrator.
8. Tab to the *Authorization Code* field and enter the authorization code you obtained from your Administrator.
9. Click *OK* in the *Create Entrust User* dialog.

   After a short period of time, a message appears confirming that your Client username was created. The Client also created your Client profile. Your profile is a file that contains critical information about you which is required by Entrust. This critical information is encrypted to ensure security. For increased security, you can store your Client profile permanently on a floppy diskette. Whenever you need to use the Client, you can access your profile via the floppy diskette. The filename of your profile is the same as your username (for example, *John Smith*).


Entrust user created.

10. Click *OK*.

    The Entrust menu bar appears at the top of your screen and the Entrust control palette appears on the desktop. See Figures 2 and 3 on page 25.

You can now encrypt, decrypt, sign, and verify files. You can also create your address book and recipient lists, specify preferences, and change your password.

If Entrust was unable to create a new user, try supplying the information again. Ensure that you enter the reference number and the authorization code in exactly the same form as you received them from your Entrust Administrator. If you still cannot create a Client username, contact your Administrator.

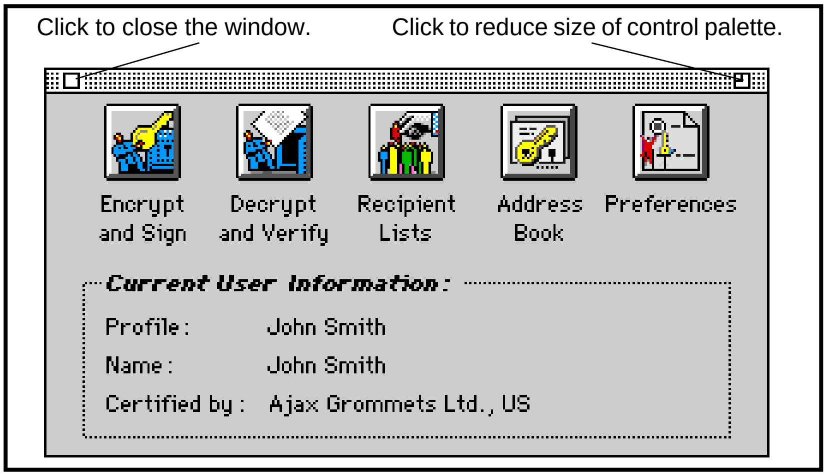
The control palette contains icons that you can click to access the main Client functions. In addition, the following information is displayed (when the palette is in full view):

- name of your Client profile

- your name
- the name of your Certification Authority

Note: The Certification Authority comprises one or more people who are responsible for security policy decisions in the organization. Entrust Security Officers and Administrators are agents of your organization’s Certification Authority.

Figure 2 Entrust control palette (full size)



Current User Information:

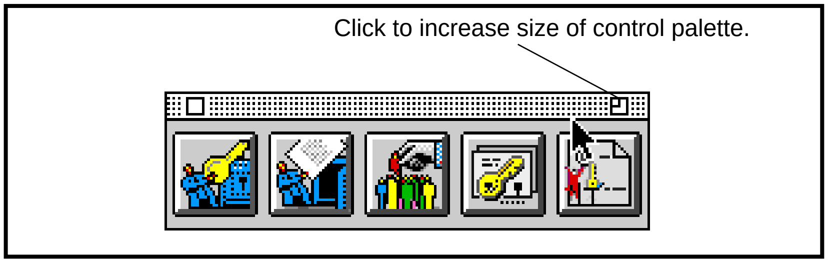
Profile: John Smith

Name: John Smith

Certified by: Ajax Grommets Ltd., US

You can close the control palette by clicking the top-left corner. You can change the size of the control palette by clicking the top-right corner.

Figure 3 Entrust control palette (reduced size)



If the control palette does not appear, you can make it visible by selecting *Control Palette...* from the *File* menu.

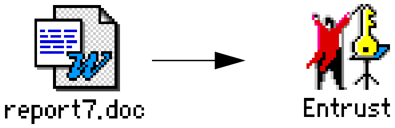
Dragging and dropping files

System 7.1

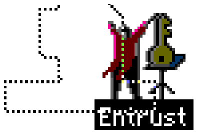
In System 7.1, the Client supports drag and drop. To start up the Client by dragging and dropping files or folders, proceed as follows:

1. Select one or more files (or folders) on the desktop in the Finder. Do not release the mouse button.

2. While holding down the mouse button, drag the selected file(s) to the *Entrust* icon or its alias.



3. When the *Entrust* icon becomes selected (it becomes darker), release the mouse button.



> ***Note:*** Ensure that you release the mouse button only when the *Entrust* icon is selected; otherwise, the file you dragged and dropped will remain on the desktop and the Client will not start up.

The appropriate Client dialog will appear. For example, if you drag unprotected files and drop them on the *Entrust* icon, the *Encrypt & Sign* dialog will appear. Similarly, if you drag files that were already protected using Entrust and drop them on the *Entrust* icon, the *Decrypt & Verify* dialog will appear.

If you drag a folder to the *Entrust* icon that contains both protected and unprotected files, the unprotected files will be displayed in the *Encrypt & Sign* dialog and the protected files will be displayed in the *Decrypt & Verify* dialog.

If you are not logged on to the Client, you will be prompted to log on.

System 7.5

In System 7.5, you can also drag and drop files and folders to the Entrust icon. In addition, you can drag and drop files and folders to the appropriate control palette icon or dialog. For example, you can drag and drop an unprotected file to the *Encrypt and Sign* icon on the control palette or to the *Encrypt & Sign* dialog if it is already displayed.

Similarly, you can drag and drop a protected file to the *Decrypt and Verify* icon on the control palette or to the *Decrypt & Verify* dialog box if it is already displayed.

Encrypting and signing your first file

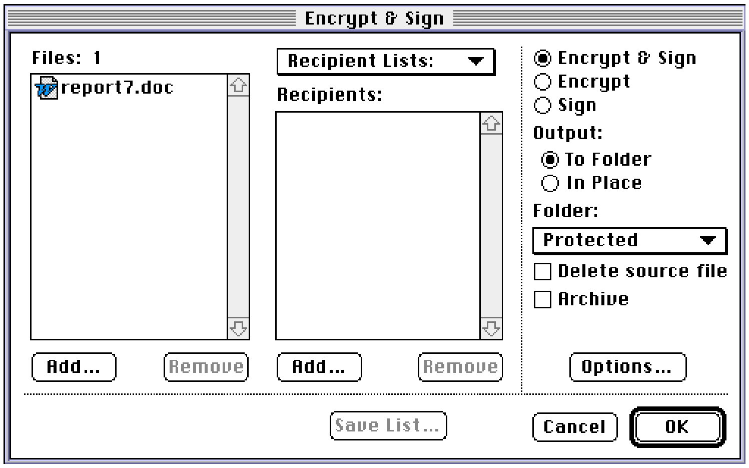
There are a number of ways to encrypt and sign files. This section shows you how to encrypt and sign a single file by dragging it from the desktop in the Finder to the *Entrust* icon. The procedure for encrypting and signing multiple files is very similar.

It is assumed that you are logged on to the Client; however, it is possible that you were automatically logged off. The Client has a safety feature that logs you off a preset number of minutes after you last used the Client. To change the preset number of minutes before being automatically logged off, refer to “Other options” on page 101. If you attempt to use the Client while you are logged off, you will be prompted to log on.

Choose a file to encrypt and sign and proceed as follows:

1. From the desktop, select the file you want to encrypt and sign, and drag it to Entrust. Refer to “Dragging and dropping files” on page 26 for information about dragging and dropping files.

   The *Encrypt & Sign* dialog appears displaying the name of the file you dragged and dropped to Entrust (for example, report7.doc).



Encrypt & Sign

Files: 1

report7.doc

Recipient Lists:

Recipients:

● Encrypt & Sign
○ Encrypt
○ Sign

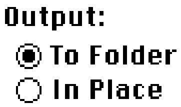
Output:
● To Folder
○ In Place

Folder: Protected

□ Delete source file
□ Archive

2. Notice that the *Encrypt & Sign* option is already selected. This means that the selected file will be both encrypted and signed.

3. Notice the *Output* radiobuttons.



Output:

● To Folder

○ In Place

The *Output* radiobuttons determine where the protected files will be stored. Valid settings are as follows:

- To Folder
- In Place

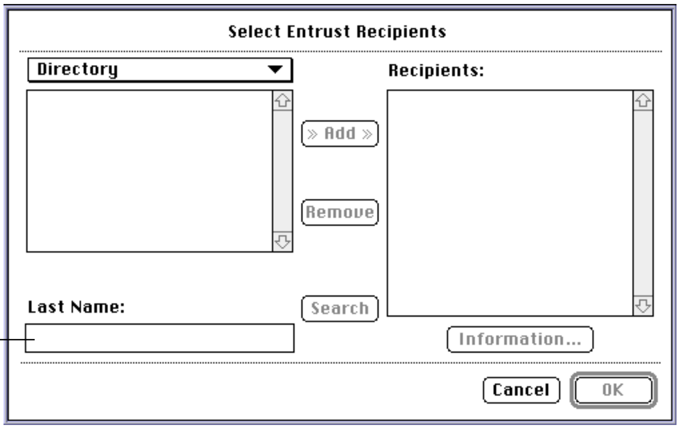
Select *To Folder* to store the protected files in the folder specified in the *Folder* pull-down menu. This folder selection remains in effect until you change it. The *Folder* pull-down menu only appears if *Output* is set to *To Folder*. Click the *Folder* pull-down menu to view the complete path to the folder. Choose *New Destination…* in the pull-down menu to change the folder.

Select *In Place* to store the protected files in the same folders as the original unprotected files. This option will also work if you select files from different folders.

Note that the original, unprotected files are left intact.

4. Click the *Add…* button under the *Recipients* section of the *Encrypt & Sign* dialog.

The *Select Entrust Recipients* dialog appears.



Search field

5. Locate the search field(s) within *Select Entrust Recipients* dialog.

If no search field appears in the dialog, it is probably because you do not have a network connection. For more information about this situation, refer to “Search information is unavailable” on page 114.

ATTENTION

The search field(s) can vary from organization to organization. Therefore, the search field(s) you see will be those that are most useful for searching the names of recipients in your organization. In this user guide, a single search field (*Last Name*) is used. If you do not know how to use the search field(s), ask your Entrust Administrator.

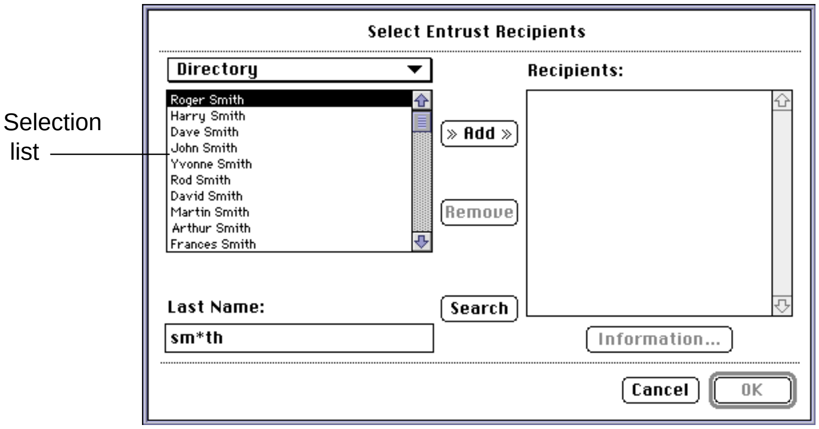
6. In the search field(s), enter the name of one or more people to whom you want to give protected file(s).

   You can replace characters with the * wild card (for example, sm*th would find occurrences of smith, smooth and smyth).

7. Press the *return* key or click *Search*.

   Note: In this dialog, you can press the *return* key instead of clicking the *Search* button and you can press the *enter* key instead of clicking the *OK* button.

The result of the search appears in the selection list.



Roger Smith
Harry Smith
Dave Smith
John Smith
Yvonne Smith
Rod Smith
David Smith
Martin Smith
Arthur Smith
Frances Smith

Last Name: sm*th

Note: There is a limit to the number of possible recipients that can be displayed in the selection list. If the search information you specify is too broad, this limit may be exceeded and only a partial list of recipients will be displayed in the selection list. A message will alert you to this situation. If this occurs, return to step 6. and enter more specific search information (for example, if you had entered s* in the search field, you might then enter sm*th instead).

8. Select the names of the recipients you want from the selection list and click >> *Add* >>. Alternatively, you can double-click the names of the recipients you want.

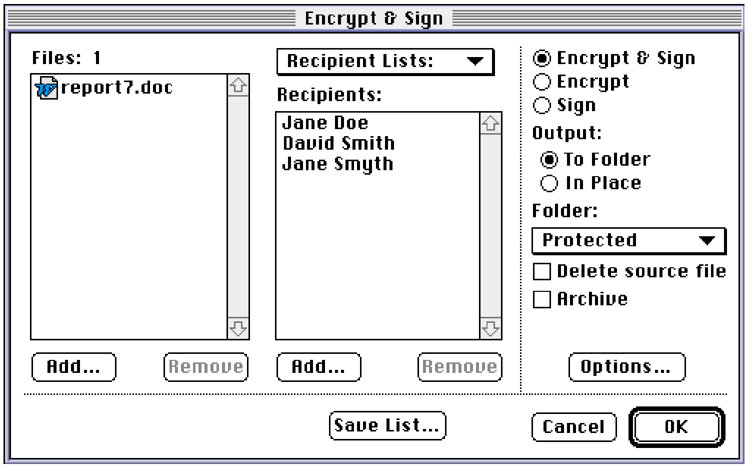
The names of the people you select from the selection list appear in the *Recipients* section. These are the people who are authorized to decrypt the file you are about to encrypt.

9. You can remove names from the *Recipients* section by double-clicking each one individually. Alternatively, you can select the names you want to remove and click the *Remove* button.

10. If want to search for more recipients, return to step 6.

11. Once you have selected all the recipients you want, click *OK* to leave the *Select Entrust Recipients* dialog. Alternatively, you can press the *enter* key.

12. The *Encrypt & Sign* dialog reappears displaying the selected recipients in the *Recipients* section. You can remove recipients by selecting their names and clicking the *Remove* button.



Encrypt & Sign

Files: 1

report7.doc

Recipients:

Jane Doe
David Smith
Jane Smyth

● Encrypt & Sign
○ Encrypt
○ Sign

Output:

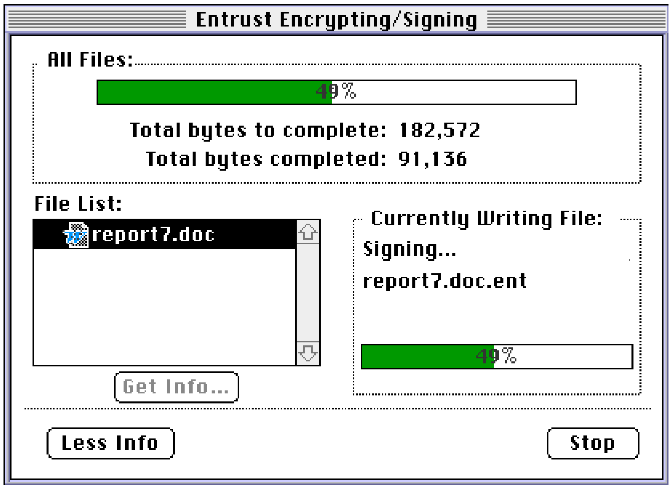
● To Folder
○ In Place

Folder: Protected

□ Delete source file
□ Archive

Once you have selected the appropriate set of recipients, click *OK* to encrypt and sign the file.

The *Entrust Encrypting/Signing* dialog appears and the file is encrypted and signed.



Total bytes to complete: 182,572
Total bytes completed: 91,136

report7.doc

Signing...
report7.doc.ent

13. To get more information about the status of a protected file, select the file name from the *File List* and click *Get Info…*

14. Click *Done* in the *Entrust Encrypting/Signing* dialog once the file is encrypted and signed.

The file you dragged and dropped to Entrust is now securely encrypted and signed, and is stored in the folder you specified in the *Encrypt & Sign* dialog. If you look in that folder, you will notice that the file you encrypted has a *.ent* filename suffix (for example, if you protect the file *report7.doc*, the filename of the protected file would be *report7.doc.ent*).

You can now give the protected file to your chosen recipients. No one other than the chosen recipients and you will be able to decrypt the file.

You will notice a slight increase in the size of files after you encrypt and/or sign them. The size of a protected file varies depending on whether the file is only encrypted, only signed, or both encrypted and signed. The size of the protected file increases slightly for each recipient you include.

ATTENTION

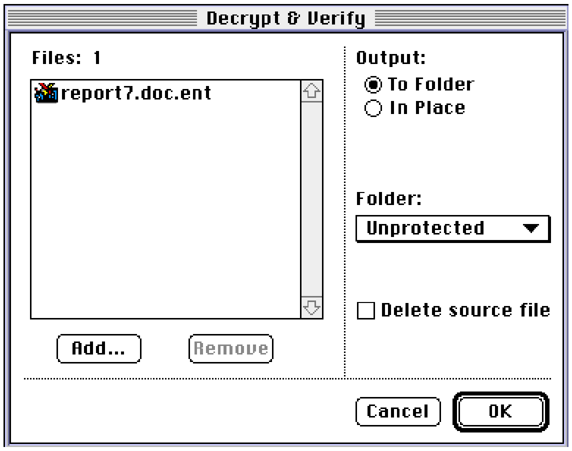
It is critical that you do not make changes to protected files. Even the slightest change to the files will cause corruption and make it impossible to decrypt and verify them at a later time.

Decrypting and verifying your first protected file

In this section, you will decrypt and verify the file you just encrypted and signed. Proceed as follows:

1. Select the file you just encrypted (for example, *report7.doc.ent*) and drag it to Entrust. Refer to “Dragging and dropping files” on page 26 for information about dragging and dropping files.

   The *Decrypt & Verify* dialog appears.



Decrypt & Verify

Files: 1

report7.doc.ent

Output:

● To Folder

○ In Place

Folder: Unprotected

□ Delete source file

2. Notice the *Output* radiobuttons.

   The *Output* radiobuttons determine where the unprotected files will be stored. Valid settings are as follows:

   - To Folder
   - In Place

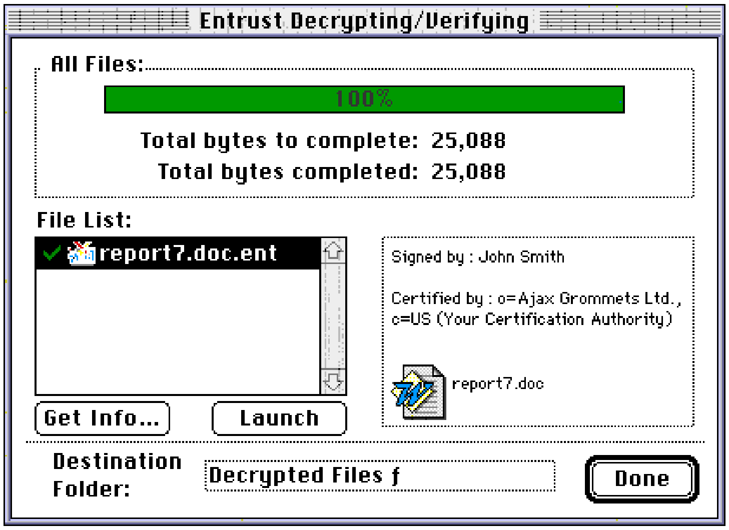
   Select *To Folder* to store the unprotected files in the folder specified in the *Folder* pull-down menu. This folder selection remains in effect until you change it. The *Folder* pull-down menu only appears if *Output* is set to *To Folder*. Click the *Folder* pull-down menu to view the complete path to the folder. Choose *New Destination…* in the pull-down menu to change the folder.

   Select *In Place* to store the unprotected files in the same folders as the original protected files. This option will also work if you select files from different folders.

   Note that the original, protected files are left intact.

3. Click *OK*.

The *Entrust Decrypting/Verifying* dialog appears.



Entrust Decrypting/Verifying

All Files:

100%

Total bytes to complete: 25,088

Total bytes completed: 25,088

File List:

✓ report7.doc.ent

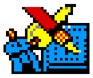
Signed by : John Smith

Certified by : o=Ajax Grommets Ltd., c=US (Your Certification Authority)

report7.doc

Destination Folder: Decrypted Files ƒ

The filename appears in the *File List* and a check mark appears beside the filename indicating that the file was successfully processed. The icon next to the filename indicates that the file was encrypted and signed.



The name of the person who signed the file is shown in the *Signed by* field to the right of the *File List*.

4. To get more information about the status of the unprotected file, select the file in the *File List* and click *Get Info…*

5. The name and icon of the unprotected file appear to the right of the *File List*. To launch the unprotected file, double-click the file in the *File List*. Alternatively, you can select the name of the file in the *File List* and click *Launch*.

6. Click *Done* to leave the dialog.

   Your file is now decrypted and verified.

The decrypted file is stored in the folder specified in the *Destination Folder* field.

Ending your Entrust/Client session

To end your Client session, choose *Quit* from the *File* menu.

Using Entrust/Client

This chapter provides step-by-step procedures for Entrust/Client functions. Most of these procedures assume the following:

- The Client was successfully installed on your computer.
- You created your Client username.
- You already started up the Client.

  Note: If the Client is not already started, refer to “Starting Entrust/Client for the first time” on page 22.

Most of the procedures in this chapter also assume that you are logged on to the Client; however, it is possible that you were automatically logged off. Entrust has a safety feature that logs you off a preset number of minutes after you last used the Client. To change the preset number of minutes before being automatically logged off, refer to “Other options” on page 101. If you attempt to use Entrust while you are logged off, you will be prompted to log on.

Protecting the contents of your files

You can protect the contents of your files from intruders by encrypting them using Entrust/Client. Once protected, these files cannot be read by anyone (including you) until they are decrypted.

You can distribute protected files to recipients of your choice with complete confidence that only the intended recipients can decrypt them.

You can provide your recipients with additional assurance by digitally signing the protected files that you give them. Your digital signature guarantees that the files came from you and that they were not altered since you sent them.

It is possible to select one or more folders to be encrypted and/or signed. You can select a folder for protection using any of the methods for dragging and dropping files on the Client (see "Dragging and dropping files" on page 26). When you select a folder for protection, all of the unprotected files within the folder (including those within subfolders) are automatically selected for protection and displayed in the *Encrypt & Sign* dialog.

To protect the contents of your files, you need to complete the following steps:

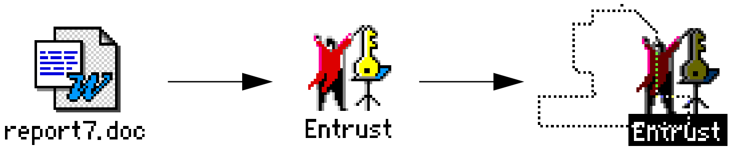
- Access the *Encrypt & Sign* dialog.
- Select the files you want to encrypt and/or sign.
- Select recipients for the encrypted files (you do not need to select recipients for files that are signed but not encrypted).
- Save current recipients and options in a recipient list. This step is optional.
- Encrypt and/or sign the files.

Each of these steps is described in detail in the following sections.

Accessing the Encrypt & Sign dialog

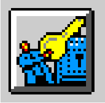
To encrypt and sign files you need to access the *Encrypt & Sign* dialog. You can do this three ways:

- Drag one or more files or folders to Entrust. Refer to “Dragging and dropping files” on page 26 for information about dragging and dropping files and folders.



> ***Note:*** You may find it convenient to store an alias of the *Entrust* icon on the desktop in the Finder to facilitate dragging and dropping files.

- Click the *Encrypt and Sign* icon on the Entrust control palette.

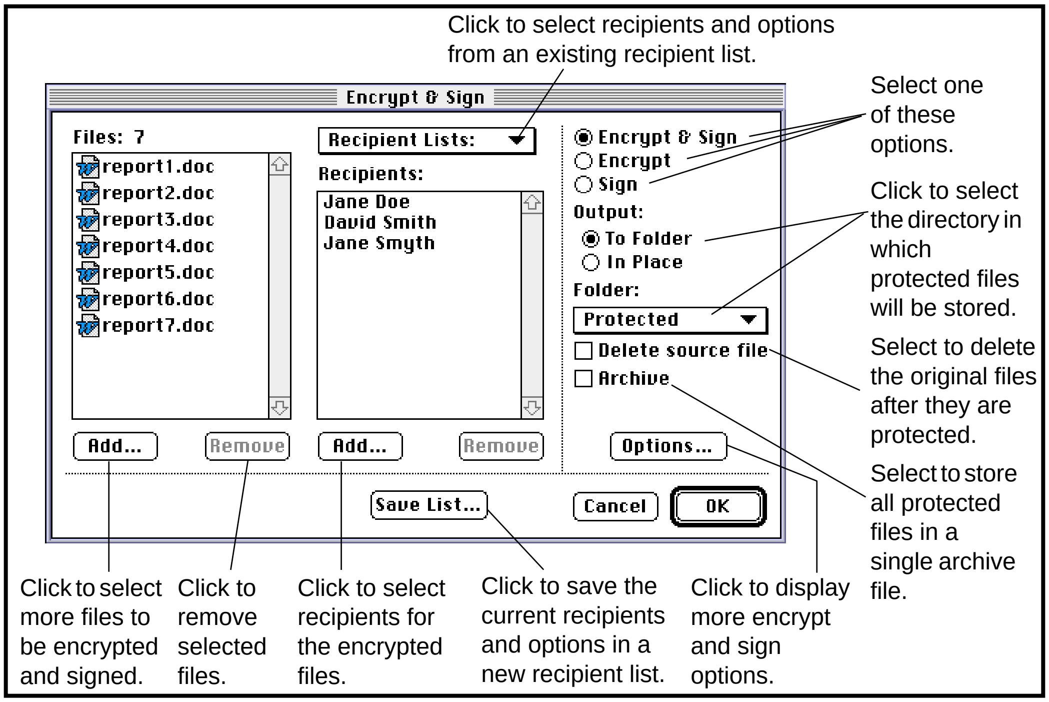


- Choose *Encrypt/Sign...* from the *File* menu.

In all cases, the *Encrypt & Sign* dialog appears (see Figure 4 on page 40).

> ***Note:*** If you are not currently logged onto the Client, you will be prompted to log on before the *Encrypt & Sign* dialog appears.

Figure 4 Encrypt & Sign dialog



Files: 7

report1.doc
report2.doc
report3.doc
report4.doc
report5.doc
report6.doc
report7.doc

Recipients:

Jane Doe
David Smith
Jane Smyth

● Encrypt & Sign
○ Encrypt
○ Sign

Output:
● To Folder
○ In Place

Folder: Protected

□ Delete source file
□ Archive

Click to select recipients and options from an existing recipient list.

Select one of these options.

Click to select the directory in which protected files will be stored.

Select to delete the original files after they are protected.

Select to store all protected files in a single archive file.

Click to select more files to be encrypted and signed.

Click to remove selected files.

Click to select recipients for the encrypted files.

Click to save the current recipients and options in a new recipient list.

Click to display more encrypt and sign options.

The *Encrypt & Sign* dialog contains the following functional sections:

- files to be encrypted and/or signed
- list of recipients for encrypted files
- options to be used when encrypting and/or signing files
- saved recipient lists

The *Encrypt & Sign* dialog serves another purpose. Once you have selected the recipients and options you want, you can click *Save List...* to save them in a *recipient list*. You give this *recipient list* a name to which you can refer later when you need to encrypt more files for the same set of recipients using the same set of options. Later, you can also make changes to this *recipient list*. For more information about recipient lists, refer to “Using saved lists of recipients” on page 80.

Selecting files you want to encrypt and sign

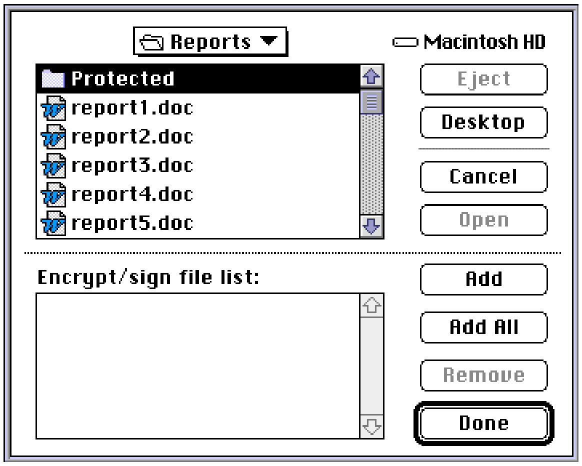
This section describes how to select the files you want to encrypt and/or sign. Each of the files you select for protection is encrypted for the same set of recipients.

If you displayed the *Encrypt & Sign* dialog by dragging unprotected files or folders to Entrust, the files you selected already appear in the *Files* section of the *Encrypt & Sign* dialog (see Figure 4).

To add files to the list of files to be encrypted and/or signed, proceed as follows:

1. Click *Add*... in the *Encrypt & Sign* dialog.

The following dialog appears.

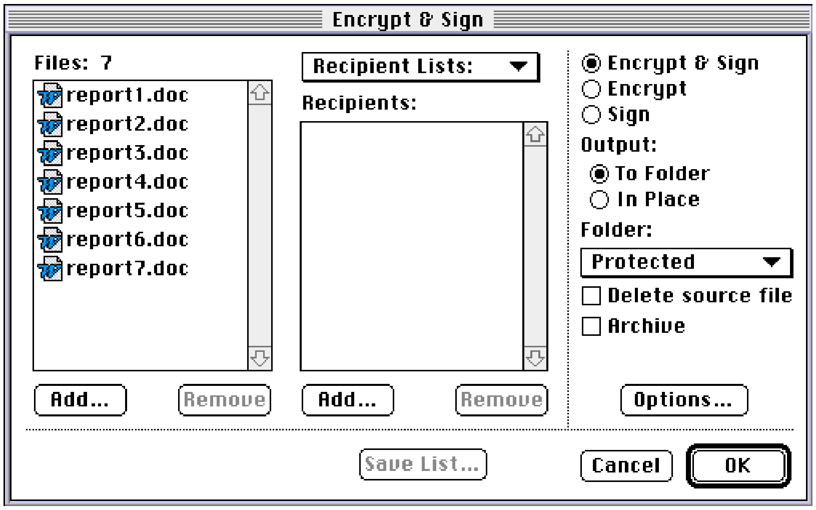


2. Navigate to the folder that contains the file(s) you want to encrypt and/or sign.

3. Select a single file you want to protect by double-clicking it. Alternatively, you can select a single file and then click *Add*. Click *Add All* to add all of the files from the current directory to the *Encrypt/sign file list*.

4. When you have selected the files for protection, click *Done* to return to the *Encrypt & Sign* dialog.

The *Encrypt & Sign* dialog reappears displaying the files you selected.



Encrypt & Sign

Files: 7

- report1.doc
- report2.doc
- report3.doc
- report4.doc
- report5.doc
- report6.doc
- report7.doc

Recipient Lists:

Recipients:

● Encrypt & Sign
○ Encrypt
○ Sign

Output:
● To Folder
○ In Place

Folder: Protected

□ Delete source file
□ Archive

5. Repeat steps 1. through 3. until you have selected all the files you want to protect. You can select files from more than one directory.

> ***Note:*** To specify files for protection, you can also select unprotected files (or folders) in the Finder and drag and drop those files directly onto the *Files* section of the *Encrypt & Sign* dialog.

Now you should select recipients for your encrypted files. Refer to “Selecting recipients for your encrypted files” below for more information. If you want to encrypt a file so that only you can decrypt it, you do not need to select any recipients. Also, if you only want to sign files, you do not need to select recipients. In those cases, refer to “Selecting encrypting and signing options” on page 58 for information about selecting options.

Selecting recipients for your encrypted files

Recipients are the people whom you authorize to decrypt your protected files. You only need to select recipients for encrypted files. If you sign files without encrypting them, there is no need to specify recipients. Note that you are automatically designated as a recipient for each file you encrypt; therefore, you do not have specify yourself as a recipient.

You can select recipients for encrypted files in the following ways:

- by selecting an existing recipient list from the *Encrypt and Sign* dialog (see “Selecting an existing recipient list from the Encrypt and Sign dialog” on page 53)
- by selecting an existing recipient list from the *Select Entrust Recipients* dialog (see “Selecting an existing recipient list from the Select Entrust Recipients dialog” on page 55)
- by searching for the names of people (see “Selecting recipients by name” on page 44)
- by selecting people from your address book (see “Selecting recipients by name in personal address book” on page 49)
- any combination of the above

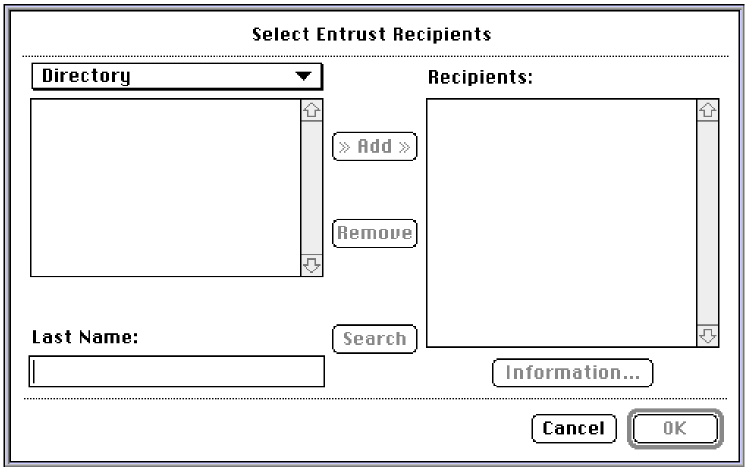
Selecting recipients by name

This section assumes the *Encrypt & Sign* dialog is displayed. If it is not, refer to “Accessing the Encrypt & Sign dialog” on page 39.

To select recipients by name, proceed as follows:

1. Click *Add...* at the bottom of the *Recipients* section in the *Encrypt & Sign* dialog.

   The *Select Entrust Recipients* dialog appears.



2. Select *Directory* from the pull-down list at the top of the *Select Entrust Recipients* dialog.
3. Locate the search field(s) to the left of the *Search* button.

   If no search field appears in the dialog, it is probably because you do not have a network connection. If you do not have a network connection, the contents of your address book (if you have one) will appear automatically in the selection list. For more information about this situation, refer to “Search information is unavailable” on page 114.

ATTENTION

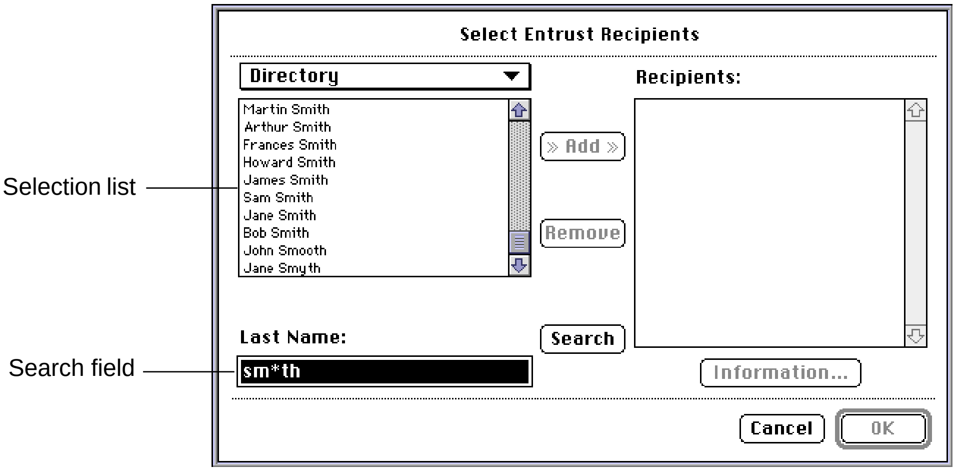
The search field(s) can vary from organization to organization. Therefore, the search field(s) you see will be those that are most useful for searching the names of recipients in your organization. In this user guide, a single search field (*Last Name*) is used. If you do not know how to use the search field(s), ask your Entrust Administrator.

4. In the search field(s), enter the name of a person to whom you want to give protected files.

You can replace characters in the search field(s) with the * wild card; for example, sm*th would find occurrences of smith, smooth and smyth.

5. Press the *Return* key or click the *Search* button.

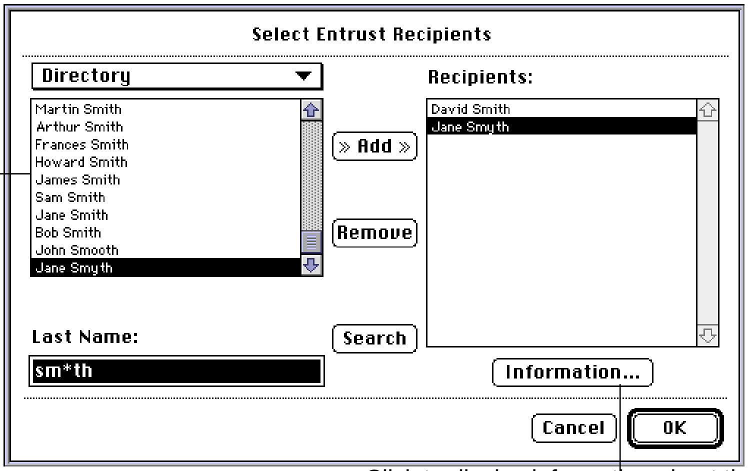
   The result of the search appears in the selection list.



Note: There is a limit to the number of possible recipients that can be displayed in the selection list. If the search information you specify is too broad, this limit may be exceeded and only a partial list will be displayed in the selection list. A message will alert you to this situation. If this occurs, return to step 4. and enter more specific search information (for example, if you had entered s* in the search field, you might then enter sm*th instead). If there is heavy traffic on your network, it is possible that the search may take too long (such occurrences are rare, however). You can cancel the search by holding down the *Command* and period keys at the same time.

6. Select the names of the recipients you want from the selection list and click *>> Add >>*. Alternatively, you can double-click the names of the recipients you want.

The names of the recipients you select from the selection list appear in the *Recipients* section of the *Select Entrust Recipients* dialog. These are the people who are authorized to decrypt the files you are about to encrypt.

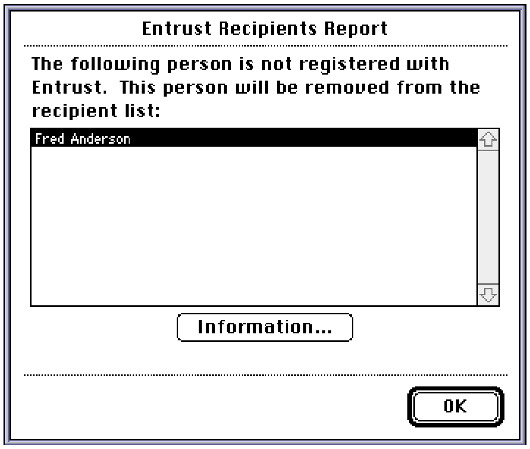


Last Name: sm*th

Selection list

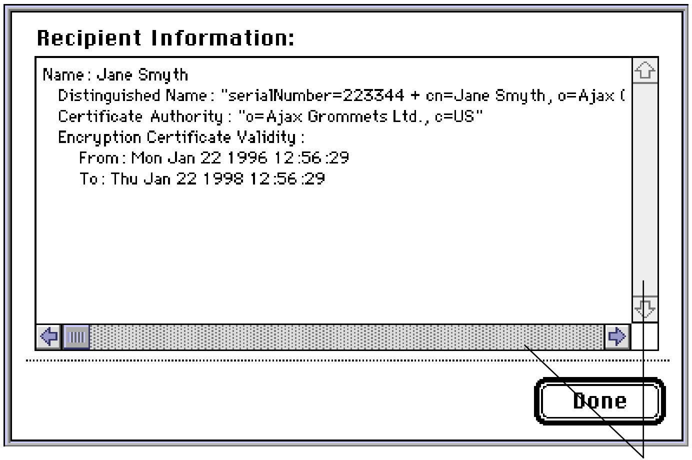
Click to display information about the currently selected recipient.

Note: If the *Entrust Recipients Report* dialog appears when you select names from the selection list, it means that the Client cannot encrypt files for the recipient shown in the dialog. Click *OK* and continue the procedure. If you want to know why the Client cannot encrypt files for a rejected recipient, select the recipient's name and click *Information…*. Click *OK* to leave the *Entrust Recipients Report* dialog.



The following person is not registered with Entrust. This person will be removed from the recipient list:

7. You can display information about a recipient by selecting the recipient's name and clicking *Information*... in the *Select Entrust Recipients* dialog.



Recipient Information:

```
Name : Jane Smyth
  Distinguished Name : "serialNumber=223344 + cn=Jane Smyth, o=Ajax (
  Certificate Authority : "o=Ajax Grommets Ltd., c=US"
  Encryption Certificate Validity :
     From : Mon Jan 22 1996 12:56:29
     To : Thu Jan 22 1998 12:56:29
```

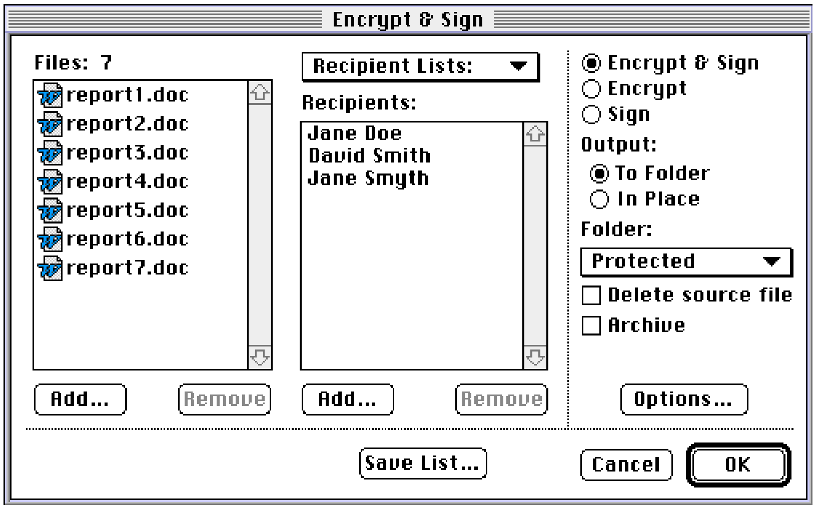
Use the scroll bars to view all of the information.

8. You can remove recipients individually from the *Recipients* section of the *Select Entrust Recipients* dialog by double-clicking them.

9. If you want to include more recipients by name, return to step 4.

10. Once you have selected all the recipients you want, click *OK* (or hit the *enter* key) to leave the *Select Entrust Recipients* dialog.

The *Encrypt & Sign* dialog reappears displaying the names of the recipients you selected.



Encrypt & Sign

Files: 7

report1.doc
report2.doc
report3.doc
report4.doc
report5.doc
report6.doc
report7.doc

Recipients:

Jane Doe
David Smith
Jane Smyth

● Encrypt & Sign
○ Encrypt
○ Sign

Output:

● To Folder
○ In Place

Folder: Protected

□ Delete source file
□ Archive

11. You can add more recipients using one of the methods explained in “Selecting recipients for your encrypted files” on page 43.

    You can remove recipients from the *Recipients* section of the *Encrypt & Sign* dialog by selecting the recipients you want to remove and clicking *Remove*.

Now you can specify encrypting and signing options. Refer to “Selecting encrypting and signing options” on page 58 for more information.

Selecting recipients by name in personal address book

This section assumes the *Encrypt & Sign* dialog is displayed. If it is not, refer to “Accessing the Encrypt & Sign dialog” on page 39.

You can specify recipients by selecting names from your personal address book.

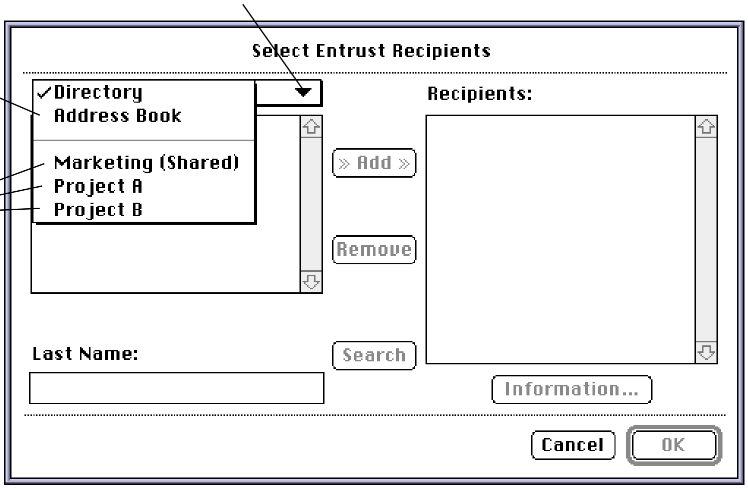
To select recipients from your address book, proceed as follows:

1. Click *Add*... at the bottom of the *Recipients* section in the *Encrypt & Sign* dialog.

   The *Select Entrust Recipients* dialog appears.

2. Select *Personal Address Book* from the pull-down list at the top of the *Select Entrust Recipients* dialog.

Click arrow to select *Personal Address Book*.

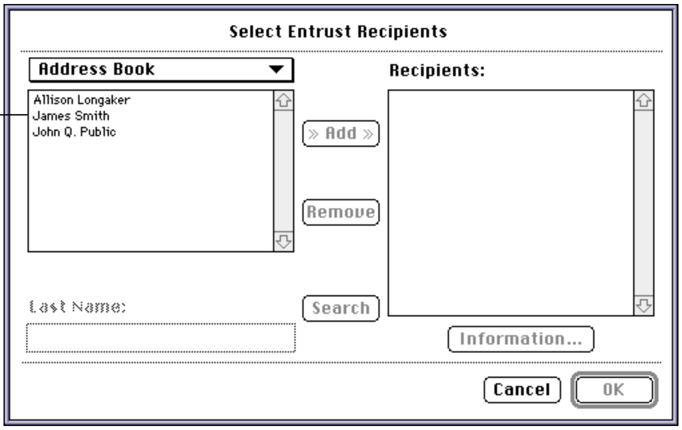


Address Book only appears if you already created it.

Recipient lists only appear if you already created some.

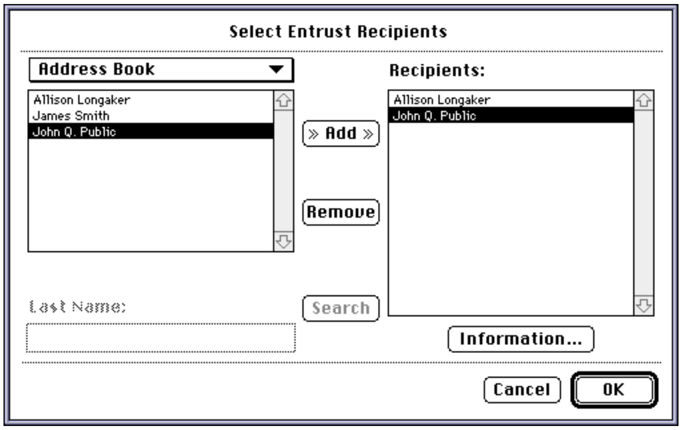
Note: If *Personal Address Book* does not appear in the pull-down list at the top of the *Select Entrust Recipients* dialog, you have not yet created an address book. For information about address books, refer to “Creating and accessing your address book” on page 72.

The names in your address book appear in the selection list.

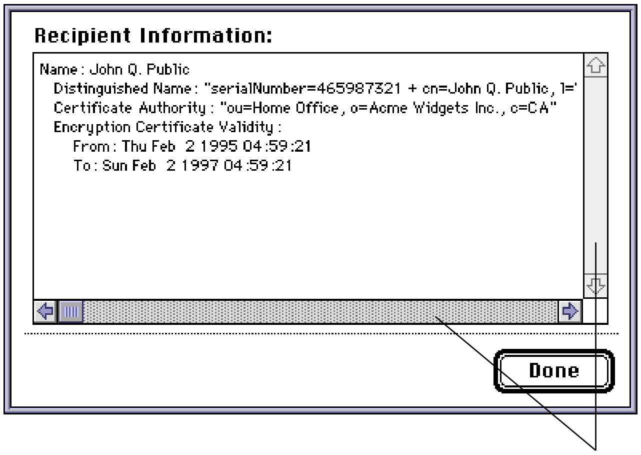


3. Select the names of the recipients you want from the selection list and click *>> Add >>*. Alternatively, you can double-click the names of the recipients you want.

   The names of the recipients you select from the selection list appear in the *Recipients* section of the *Select Entrust Recipients* dialog. These are the people who are authorized to decrypt the files you are about to encrypt.



4. You can display information about a recipient by selecting the recipient’s name and clicking *Information*...



Recipient Information:

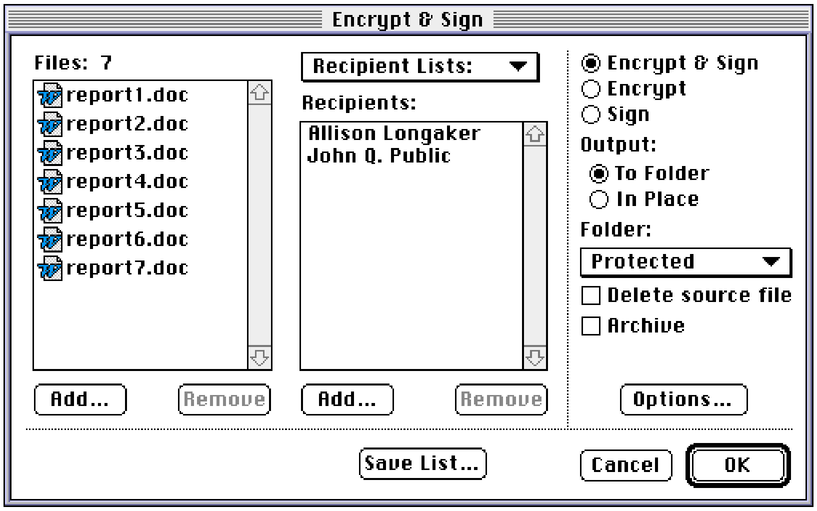
```
Name : John Q. Public
   Distinguished Name : "serialNumber=465987321 + cn=John Q. Public, 1='
   Certificate Authority : "ou=Home Office, o=Acme Widgets Inc., c=CA"
   Encryption Certificate Validity :
       From : Thu Feb  2 1995 04:59:21
       To : Sun Feb  2 1997 04:59:21
```

Use the scroll bars to view
all of the information.

5. You can remove recipients individually from the *Recipients* section of the *Select Entrust Recipients* dialog by double-clicking them.

6. Once you have selected all the recipients you want, click *OK* to leave the *Select Entrust Recipients* dialog.

The *Encrypt & Sign* dialog reappears displaying the names of the recipients you selected.



Files: 7

report1.doc
report2.doc
report3.doc
report4.doc
report5.doc
report6.doc
report7.doc

Recipients:

Allison Longaker
John Q. Public

● Encrypt & Sign
○ Encrypt
○ Sign

Output:

● To Folder
○ In Place

Folder: Protected

□ Delete source file
□ Archive

7. You can add more recipients using one of the methods explained in “Selecting recipients for your encrypted files” on page 43.

   You can remove recipients from the *Recipients* section of the *Encrypt & Sign* dialog by selecting the recipients you want to remove and clicking *Remove*.

Now you can specify encrypting and signing options. Refer to “Selecting encrypting and signing options” on page 58 for more information.

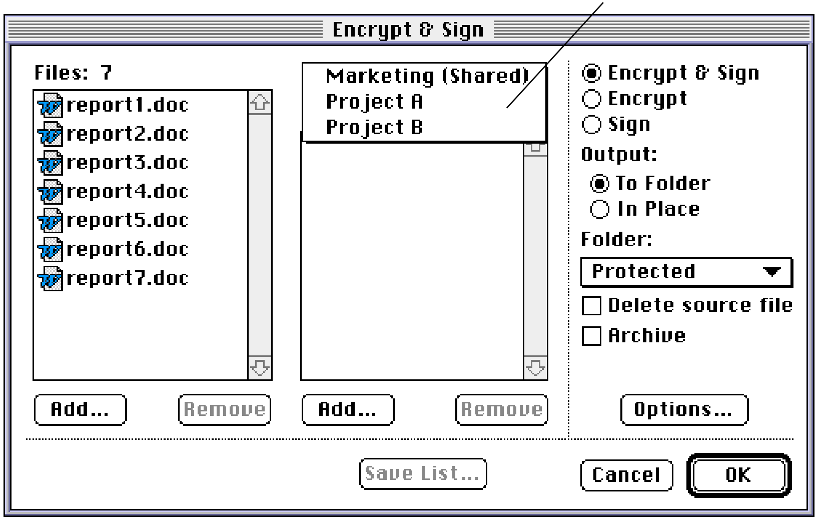
Selecting an existing recipient list from the Encrypt and Sign dialog

This section assumes the *Encrypt and Sign* dialog is displayed. If it is not, refer to "Accessing the Encrypt & Sign dialog" on page 39. This section also assumes that you have already created at least one recipient list. If you have not yet created a recipient list, refer to "Using saved lists of recipients" on page 80.

From the *Encrypt and Sign* dialog, you can specify recipients by selecting members of one of your existing recipient lists. Proceed as follows:

1. Select the name of the recipient list you want from the *Recipient Lists* pull-down list at the top of the *Encrypt and Sign* dialog.

Click to select a recipient list (if you previously created one).



Note: If no recipient lists appear in the *Recipient Lists* pull-down list, you have not yet created a recipient list. For information about recipient lists, refer to "Using saved lists of recipients" on page 80.

The names of the people who are members of the recipient list you selected appear in the *Recipients* section of the *Encrypt & Sign* dialog. These are the people who are authorized to decrypt the files you are about to encrypt.

Notice that some options may have changed in the *Encrypt & Sign* dialog when you selected a recipient list because recipient lists store a set of recipient names and options.

> ***Note:*** If the *Rejected Recipients* dialog appears when you select a shared recipient list, it is likely that some of the recipients in the shared recipient list came from the recipient list originator's personal address book. Before you can encrypt files for those recipients, you must import their Entrust addresses into your own personal address book.

2. You can add more recipients using one of the methods explained in "Selecting recipients for your encrypted files" on page 43.

You can remove recipients from the *Recipients* section of the *Encrypt & Sign* dialog by selecting the recipients you want to remove and clicking *Remove*.

If you make changes to the recipients or to the options, you can save them in a new recipient list by clicking *Save List…* at the bottom of the *Encrypt & Sign* dialog.

Now you can specify encrypting and signing options. Refer to "Selecting encrypting and signing options" on page 58 for more information.

Selecting an existing recipient list from the Select Entrust Recipients dialog

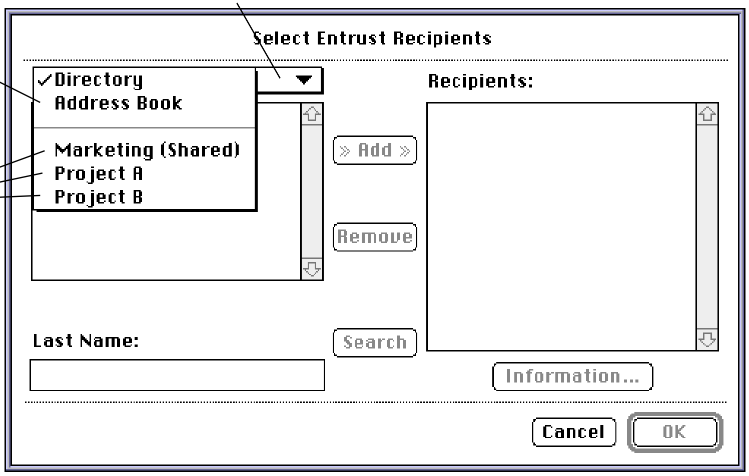
This section assumes the *Encrypt and Sign* dialog is displayed. If it is not, refer to “Accessing the Encrypt & Sign dialog” on page 39. This section also assumes that you have already created at least one recipient list. If you have not yet created a recipient list, refer to “Using saved lists of recipients” on page 80.

From the *Select Entrust Recipients* dialog, you can specify recipients by selecting members of one of your existing recipient lists. Proceed as follows:

1. Click *Add...* at the bottom of the *Recipients* section in the *Encrypt and Sign* dialog.

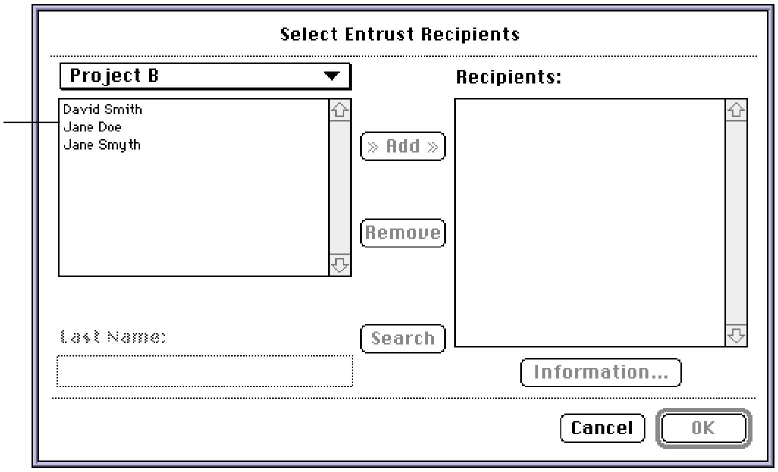
The *Select Entrust Recipients* dialog appears.

2. Select the name of the recipient list you want from the pull-down list at the top of the *Select Entrust Recipients* dialog.


Click arrow to select a recipient list.
Address Book only appears if you already created it.
Recipient lists only appear if you already created some.
Select Entrust Recipients
✓Directory
Address Book
Marketing (Shared)
Project A
Project B
Recipients:
» Add »
Remove
Search
Last Name:
Information...
Cancel
OK

Note: If no recipient lists appear in the pull-down list, you have not yet created a recipient list. For information about recipient lists, refer to “Using saved lists of recipients” on page 80.

The names of the people who are members of the recipient list you selected appear in the selection list.



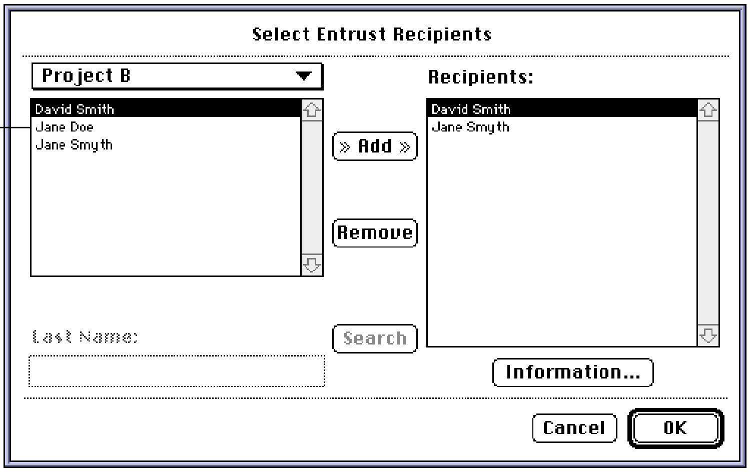
Project B

David Smith
Jane Doe
Jane Smyth

Selection list

3. Select the names of the recipients you want from the selection list and click *>> Add >>*. Alternatively, you can double-click the names of the recipients you want.

   The names of the recipients you select from the selection list appear in the *Recipients* section of the *Select Entrust Recipients* dialog. These are the people who are authorized to decrypt the files you are about to encrypt.



Project B

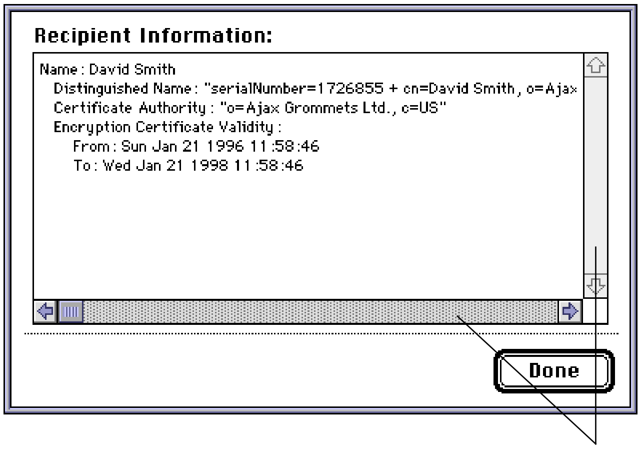
David Smith
Jane Doe
Jane Smyth

Recipients:

David Smith
Jane Smyth

Selection list

4. You can display information about a recipient by selecting the recipient’s name and clicking *Information*...



```
Name : David Smith
  Distinguished Name : "serialNumber=1726855 + cn=David Smith, o=Ajax
  Certificate Authority : "o=Ajax Grommets Ltd., c=US"
  Encryption Certificate Validity :
     From : Sun Jan 21 1996 11:58:46
     To : Wed Jan 21 1998 11:58:46
```

Use the scroll bars to view
all of the information.

5. You can remove recipients individually from the *Recipients* section of the *Select Entrust Recipients* dialog by double-clicking them.

6. Once you have selected all the recipients you want, click *OK* to leave the *Select Entrust Recipients* dialog.

   The *Encrypt & Sign* dialog reappears displaying the names of the recipients you selected.

7. You can add more recipients using one of the methods explained in “Selecting recipients for your encrypted files” on page 43.

   You can remove recipients from the *Recipients* section of the *Encrypt & Sign* dialog by selecting the recipients you want to remove and clicking *Remove*.

   If you make changes to the recipients or to the options, you can save them in a new recipient list by clicking *Save List…* at the bottom of the *Encrypt & Sign* dialog.

Now you can specify encrypting and signing options. Refer to “Selecting encrypting and signing options” on page 58 for more information.

Selecting encrypting and signing options

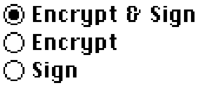
Once you have selected files to be protected and recipients (if necessary), you can choose options. If you selected a recipient list from the *Encrypt & Sign* dialog, then the options are automatically set; however, you can change those settings for this particular encrypt and/or sign operation.

This section assumes the *Encrypt & Sign* dialog is displayed. If it is not, refer to “Accessing the Encrypt & Sign dialog” on page 39.

When you select options, they remain selected until you change them again; Entrust remembers the settings you specify. However, option settings may change when you select a recipient list because recipient lists store recipient names and options.

To select encrypting and signing options, proceed as follows:

1. From the *Encrypt & Sign* dialog, select one of the following options:



● Encrypt & Sign
○ Encrypt
○ Sign

Select *Encrypt & Sign* to encrypt and sign the selected files.

Select *Encrypt* to encrypt the selected files without including your signature.

Select *Sign* to include your signature with the selected files. The files will not be encrypted. You would select this option if you were sending out information that is well known (hence it does not need to be encrypted), but you want your recipients to be assured that the information originated from you and that it has not been tampered with since you signed it.

2. Notice the *Output* radio buttons.

The *Output* radiobuttons determine where the protected files will be stored. Valid settings are as follows:

- To Folder
- In Place

Select *To Folder* to store the protected files in the folder specified in the *Folder* pull-down list. This folder selection remains in effect until you change it. The *Folder* pull-down list only appears if *Output* is set to *To Folder.*

Select *In Place* to store the protected files in the same folders as the original unprotected files. This option will also work if you select files from different folders.

Note that the original, unprotected files are left intact.

3. Clicking on the *Folder* pull-down list shows the full path to the directory in which you want to store the encrypted and signed files. To select a different folder, click the *Folder* pull-down list and select the *New Destination…* option.

   The *Folder* pull-down list is only visible when *Output* is set to *To Folder*, however, the directory you specify in the *Folder* pull-down list will remain in effect until you change it again.

4. Notice the *Archive* selection box in the *Encrypt & Sign* dialog.

   Use the *Archive* option if you want to store all the encrypted and signed files in a single archive file. This is useful if you want to transfer several protected files; by storing all the protected files in a single archive file, you only need to transfer a single file. When the file is received at the intended destination and decrypted, the original files will be restored with their original filenames.

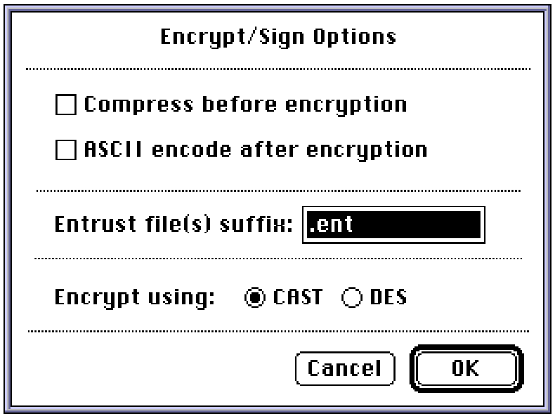
   When you select *Archive*, a data entry field appears next to the *Archive* option. Enter a filename for the archive file in the *Archive* data entry field (for example, *project1*). The *Archive* option is only available when *Output* is set to *To Folder.* The *Archive* option does not remain selected after you leave the *Encrypt & Sign* dialog.

5. Notice the *Delete source file* field in the *Encrypt & Sign* dialog.

   Select *Delete source file* to automatically delete the original files after they are protected. If you do not select this option, the original, unprotected files will remain intact after a copy of each file is protected.

6. Click *Options*... in the *Encrypt & Sign* dialog.

   The *Encrypt/Sign Options* dialog appears.



□ Compress before encryption

□ ASCII encode after encryption

Entrust file(s) suffix: .ent

Encrypt using: ● CAST ○ DES

Encrypt and sign options you can select are as follows:

- Compress before encryption
- ASCII encode after encryption
- Entrust file(s) suffix
- Encrypt using

Select *Compress before encryption* to compress the files before they are protected. It is necessary to compress files before they are encrypted because it is impossible to compress an encrypted file. By definition, an encrypted file is completely random, making compression impossible. The amount of compression depends on the type of file. Word processing files can generally be compressed to less than half their original size. Graphics files can often be compressed even more than word processing files.

Select *ASCII encode after encryption* to force Entrust to use an ASCII file format when encrypting and/or signing files. If you do not select this option, Entrust will use a binary format. One advantage of using the binary format is that the resulting size of the protected file is about 30% smaller than if you use the ASCII file format. Also, it takes less time to process files in binary format than it does to process files in ASCII file format. However, the ASCII option is mandatory if you plan to transfer the protected file using an electronic file transfer mechanism like ASCII-FTP or certain electronic mail systems that can only handle ASCII file formats.

Once your file is protected, its filename will receive the suffix specified in the *Entrust file(s) suffix* field. The default suffix is *.ent*. You can change the output file suffix by entering a different one. It is recommended that you use the default *.ent* suffix to achieve consistency among Client users across all supported platforms. Using the default also makes it easier to find protected files. For example, if you protect a file called *report7.doc*, the filename of the protected file is *report7.doc.ent*.

CAST and DES are two encryption methods available to the Client to protect your files. Typically, the decision on which to use is a policy adopted by your company or group with guidance from your Entrust Administrator.

Now you are ready to encrypt and/or sign the selected files.

Encrypting and signing files

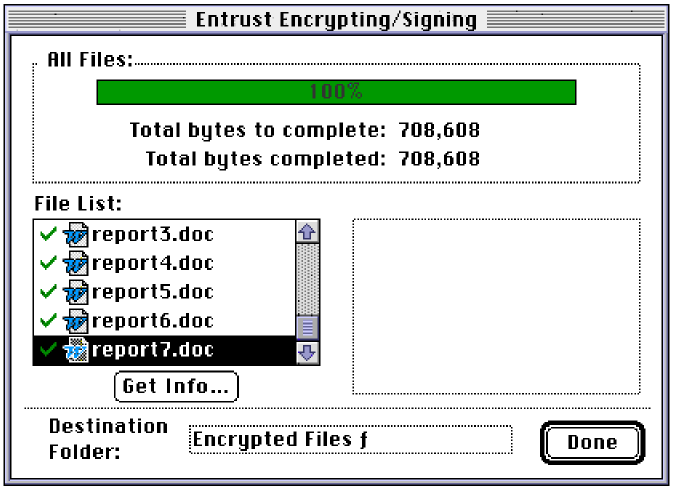
Once you have selected files to be protected, recipients (if applicable), and options, you are ready to encrypt and/or sign the selected files.

This section assumes the *Encrypt & Sign* dialog is displayed. If it is not, refer to “Accessing the Encrypt & Sign dialog” on page 39.

To encrypt and/or sign the selected files, proceed as follows:

1. Click *OK* in the *Encrypt & Sign* dialog.

   The *Entrust Encrypting/Signing* dialog appears and the files are encrypted and/or signed.



Entrust Encrypting/Signing

All Files:

100%

Total bytes to complete: 708,608

Total bytes completed: 708,608

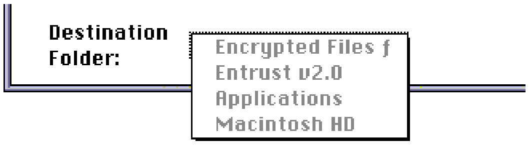
File List:

✓ report3.doc
✓ report4.doc
✓ report5.doc
✓ report6.doc
✓ report7.doc

Destination Folder: Encrypted Files ƒ

2. Notice the *Destination Folder* field.

   This field shows the name of the folder in which the protected version of the selected file in the *File List* is stored. To display the full path to that folder, hold down the *option* key and click the name of the folder.

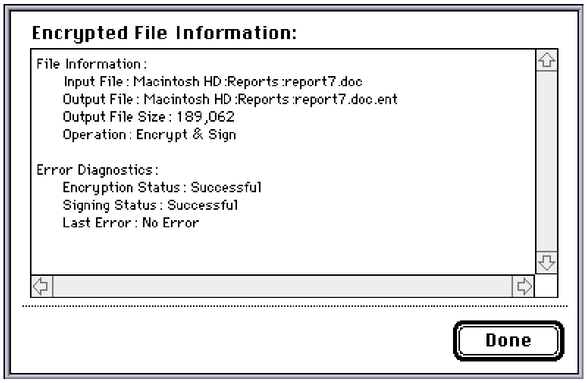


Destination Folder:

Encrypted Files ƒ
Entrust v2.0
Applications
Macintosh HD

3. To display information about the files you just protected, select a file and click *Get Info...*.

The *Encrypted File Information* dialog appears displaying information about the protected file you selected.



Encrypted File Information:

```
File Information:
     Input File: Macintosh HD:Reports:report7.doc
     Output File: Macintosh HD:Reports:report7.doc.ent
     Output File Size: 189,062
     Operation: Encrypt & Sign

Error Diagnostics:
     Encryption Status: Successful
     Signing Status: Successful
     Last Error: No Error
```

4. Click *Done* to leave the *Encrypted File Information* dialog.

   The *Entrust Encrypting/Signing* dialog reappears.

5. Click *Done* to leave the *Entrust Encrypting/Signing* dialog.

   If it is enabled, the control palette reappears.

The files you selected are now securely protected, and are stored in the folder you specified. If you look in that folder, you will notice that the files you protected have a *.ent* filename extension; for example, if you protected a file called *report7.doc*, the filename of the protected file is *report7.doc.ent*.

You can now give the protected files to your chosen recipients. No one other than the chosen recipients and you will be able to decrypt the files.

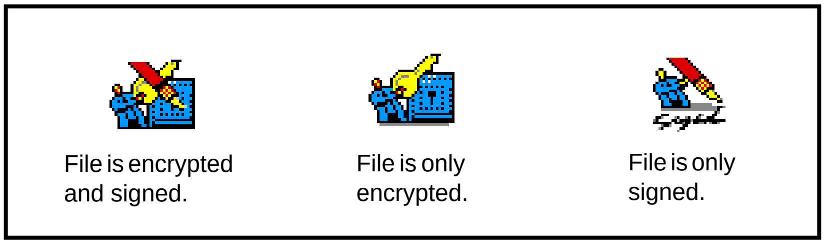
You will notice a slight increase in the size of files after you encrypt and/or sign them. The size of a protected file depends on whether the file is only encrypted, only signed, or both encrypted and signed. The size of the protected file increases slightly for each recipient you include. Use of the *Compress before encryption* and *ASCII encode after encryption* options also affects the size of protected files.

ATTENTION

It is critical that you do not make changes to protected files. Even the slightest change to the files will cause corruption and make it impossible to decrypt and verify them at a later time.

When you view protected files by icon on the desktop, they appear differently depending on whether they are encrypted, signed, or both. See Figure 5.

Figure 5 Various appearances of icons for protected files



Decrypting and verifying protected files

A protected file is a file that is encrypted, signed, or both. If a file is encrypted, you will not be able to view its contents until it is decrypted. To decrypt a file means to restore it to the state it was in just prior to being encrypted.

To verify a digital signature means to check who signed the file and to ensure the file has not been modified since it was signed. A valid digital signature is a guarantee that the file has not been altered.

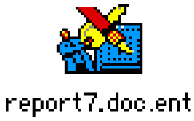
You do not have to specify whether you want to decrypt, verify, or both decrypt and verify a protected file. The Client automatically performs the appropriate operation(s) once it detects whether a protected file is encrypted, signed, or both encrypted and signed.

It is possible to select one or more folders to be decrypted and/or verified. You can select a folder for unprotection using any of the methods for dragging and dropping files on the Client (see “Dragging and dropping files” on page 26). When you select a folder for unprotection, all of the protected files within the folder (including those within subfolders) are automatically selected for unprotection and displayed in the *Decrypt & Verify* dialog.

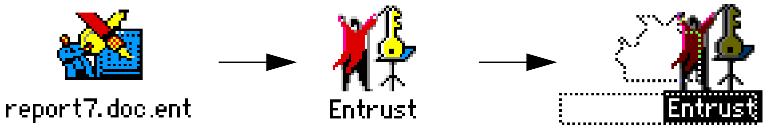
To decrypt and verify protected files, proceed as follows:

1. Access the *Decrypt & Verify* dialog using one of the following methods:

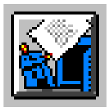
- Double-click a protected file on the desktop in the Finder (files protected by Entrust usually have the default *.ent* file suffix).



- Drag one or more protected files from the desktop in the Finder to Entrust. Refer to “Dragging and dropping files” on page 26 for information about dragging and dropping files.

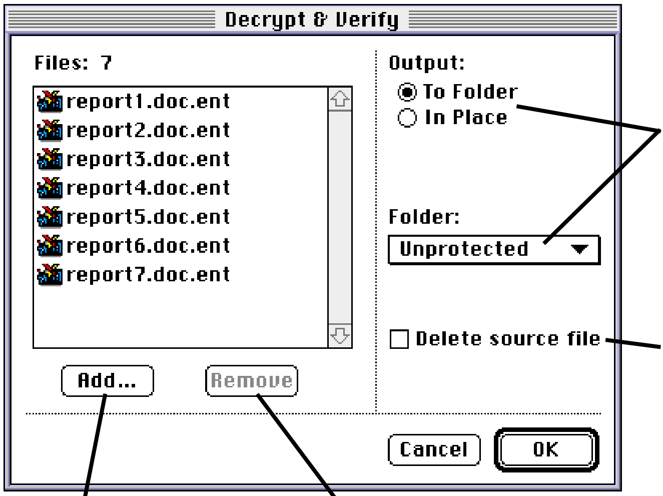


- Click the *Decrypt and Verify* icon on the control palette.



- Choose *Decrypt/Verify...* from the *File* menu.

In all cases, the *Decrypt & Verify* dialog appears. If you displayed the *Decrypt & Verify* dialog by double-clicking a protected file, or by dragging protected files or folders to Entrust, the files you selected already appear in the *Decrypt & Verify* dialog.



Click to select the folder in which unprotected files will be stored.

Select to delete the protected files after they are unprotected.

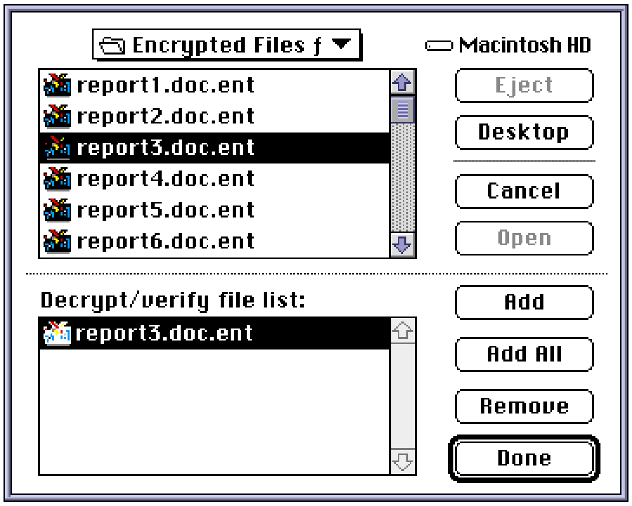
Click to select more protected files to be unprotected.

Click to remove the selected file.

2. You may select more files to unprotect. Simply drag protected files from the Finder to the *Decrypt & Verify* dialog. Alternatively, you can use the following procedure:

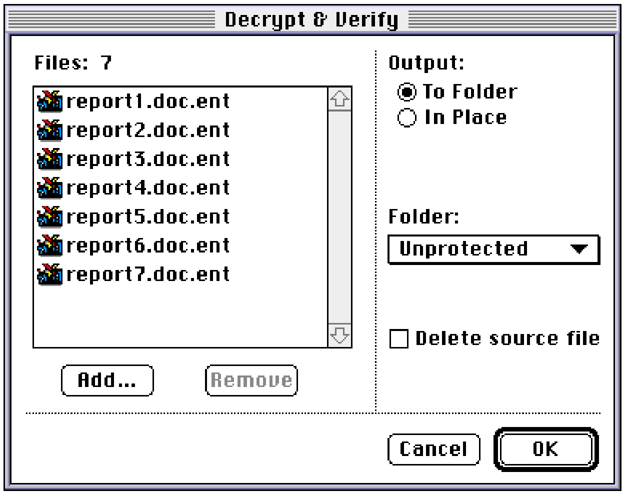
   a. Click *Add...* in the *Files* section of the *Decrypt & Verify* dialog.

The following dialog appears.



b. Select a single file you want to protect by double-clicking it. Alternatively, you can select a single file and then click *Add*. Click *Add All* to add all of the files from the current directory to the *Decrypt/verify file list*.

c. When you have selected the files for unprotection, click *Done* to return to the *Decrypt & Verify* dialog.The *Decrypt & Verify* dialog reappears displaying the files you selected.



Output:
● To Folder
○ In Place

Folder: Unprotected

□ Delete source file

d. Repeats steps 2.a to 2.c until you have selected all the files you require. You can select files from more than one folder.

Note: To specify files for unprotection, you can also select protected files (or folders) in the Finder and drag and drop those files directly onto the *Files* section of the *Decrypt & Verify* dialog.

3. Notice the *Output* radiobuttons.

The *Output* radiobuttons determine where the unprotected files will be stored. Valid settings are as follows:

- To Folder
- In Place

Select *To Folder* to store the unprotected files in a folder specified by the *Folder* pull-down list.

When you unprotect a file, the Client stores the unprotected file in the folder that you specify in the *Folder* pull-down list. This folder selection remains in effect until you change it. The *Folder* pull-down list only appears if *Output* is set to *To Folder*.

Select *In Place* to store the unprotected files in the same folders as the protected files.

Note that the protected files are left intact.

4. Clicking on the *Folder* pull-down list shows the full path to the directory in which you want to store the encrypted and signed files. To select a different folder, click the *Folder* pull-down list and select the *New Destination…* option.

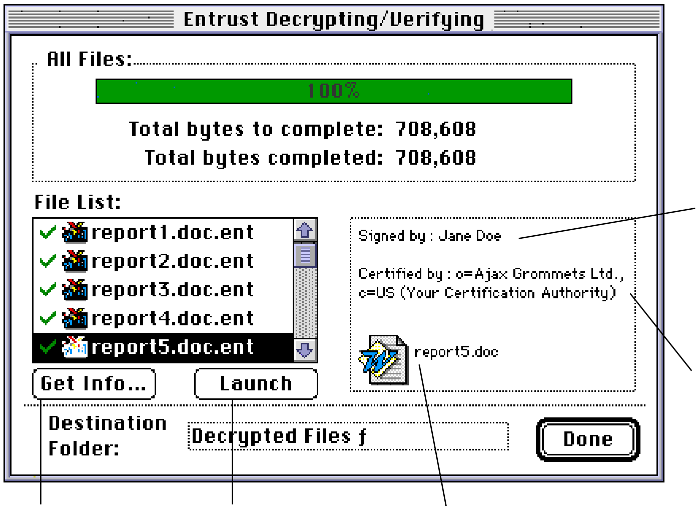
The *Folder* pull-down list is only visible when *Output* is set to *To Folder*; however, the directory you specify in the *Folder* pull-down list will remain in effect until you change it again.

5. Notice the *Delete source file* field in the *Decrypt & Verify* dialog.

Select *Delete source file* to automatically delete the original files after they are unprotected. If you do not select this option, the original, protected files will remain intact after a copy of each file is decrypted.

6. Once you have selected the files you want to unprotect, you are ready to begin the decryption and verification process. Click *OK* in the *Decrypt & Verify* dialog.

The *Entrust Decrypting/Verifying* dialog appears.



All Files:

100%

Total bytes to complete: 708,608
Total bytes completed: 708,608

File List:

- ✓ report1.doc.ent
- ✓ report2.doc.ent
- ✓ report3.doc.ent
- ✓ report4.doc.ent
- ✓ report5.doc.ent

Signed by : Jane Doe

Certified by : o=Ajax Grommets Ltd., c=US (Your Certification Authority)

report5.doc

Destination Folder: Decrypted Files ƒ

Shows the name of the person who digitally signed the file.

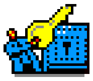
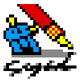
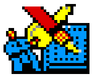
Shows the name of the Certification Authority certifying the signature.

Click to display information about the selected file.

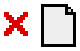
Click to view the contents of the selected file.

Shows the name and icon of the unprotected file.

The *File List* shows the files that were processed. The check mark that appears beside a filename indicates that the file was decrypted and/or verified successfully. The icons that appear beside a filename indicate whether the file was encrypted only, signed only, or both signed and encrypted.

 Indicates file was encrypted but not signed.	 Indicates file was signed but not encrypted.	 Indicates file was encrypted and signed.

Note: If either of the following icons appears instead, refer to “Symbols that indicate problems with protected files” on page 70.

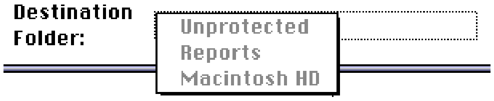


7. Notice the signature information section of the *Entrust Decrypting/Verifying* dialog. It shows the name of the person who signed the currently selected file and the name of the Certification Authority that certified the signature.

   The Certification Authority comprises one or more people who are responsible for security policy decisions in the organization.

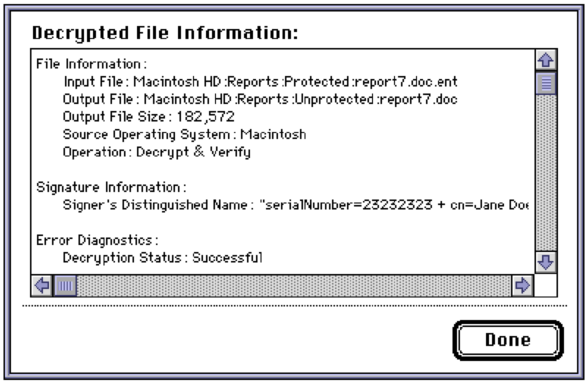
8. Notice the *Destination Folder* field.

   This field shows the name of the folder in which the unprotected version of the selected file in the *File List* is stored. To display the full path to that folder, hold down the *option* key and click the name of the folder.



9. To display information about the files you just unprotected, select one of the files and click *Get Info...*

   The *Decrypted File Information* dialog appears displaying information about the unprotected file you selected.



```
File Information :
     Input File : Macintosh HD :Reports :Protected :report7.doc.ent
     Output File : Macintosh HD :Reports :Unprotected :report7.doc
     Output File Size : 182,572
     Source Operating System : Macintosh
     Operation : Decrypt & Verify

Signature Information :
     Signer's Distinguished Name : "serialNumber=23232323 + cn=Jane Do

Error Diagnostics :
     Decryption Status : Successful
```

10. Click *Done* to leave the *Decrypted File Information* dialog.

    The *Entrust Decrypting/Verifying* dialog reappears.

11. You can view an unprotected file by double-clicking any filename in the *File List* section of the *Decrypting and Verifying* dialog. Alternatively, you can select a filename and click *Launch*. The application that was used to create the original file is launched and the file is opened. The correct version of the application must be installed on your system.

12. Click *Done* to leave the *Entrust Decrypting/Verifying* dialog.

Your files are now unprotected. You can open, move, and rename these files.

Symbols that indicate problems with protected files

If an X appears beside the filename instead of a check mark, it means that the file could not be processed.

✗ 🗋

In such a case, it is likely that the file has been damaged in transit or has been tampered with. You should ask the person who gave you the file to give you a new copy to decrypt and/or verify.

If a question mark appears with a check mark beside a filename, it means that you should not necessarily trust the signature if the file was signed.

✓?

There are two possible reasons why you should not trust the signature.

One reason is that the signing key used to sign the file is no longer valid. Ask the person who gave you the file to sign it again and to give you a new copy. Verify the new signed file to ensure the signature is valid.

The other reason why you should not trust the signature is that you do not have a network connection. As a result, Entrust could not update your Entrust signature verification information. Without access to this information, Entrust cannot fully verify that the signature used to sign the file is valid. Once you have regained access to the network, you can verify the signature with the assurance that the signature is valid. For more information about this situation, refer to “Cannot update your Entrust signature verification information” on page 113.

Exchanging protected files with Entrust users in different domains

There may be times when you want to exchange protected files with people who use Entrust in different domains.

Within the context of Entrust, a domain is a group of people who use Entrust under the same software license. Typically, these users have something in common (for example, they all work in the same company or they work on the same project).

If you want to encrypt files for someone who uses Entrust in a domain that is different from yours, you need to obtain that user’s Entrust address and associated validation string. Similarly, if you want to verify the signature on a file that came from someone who uses Entrust in a different domain, you need to obtain that user’s Entrust address and its associated validation string. If an Entrust user outside of your domain wants to encrypt files for you, you need to give that person your Entrust address and its associated validation string. Refer to “Entrust address” and “Validation string” on this page for more information.

As people give you copies of their Entrust addresses and validation strings, you should import the address information into your address book. You will not be able to exchange protected files with people who use Entrust in a domain that is different from yours unless you import their address information first. Refer to “Address book” on page 72 for more information about address books.

Entrust address

An Entrust address provides the necessary information to ensure that files encrypted and signed by someone using Entrust in one domain can be decrypted and verified by someone using Entrust used in other domains.

An Entrust address is stored in a *key* file and all users can export their own *key* file. The filename comprises your Client username with a *.key* filename suffix *(*for example, *John Smith.key*). For information about exporting your Entrust address, refer to “Exporting your personal Entrust address” on page 78.

Validation string

A validation string is a string of alphanumeric characters (for example, 7CN4-YL5D-HP7V) that is automatically generated by the Client when you export your address. Each Entrust address has a unique validation string which is associated with the *key* file. Use the validation string to confirm that the address someone gives you in a *key* file has not been tampered with since it was created.

When you export your own Entrust address in a *key* file, the associated validation string will appear in a dialog. Whenever you give someone the *key* file, also tell them the validation string. You should give people the *key* file and the validation string separately (unless you give them this information in person). Moreover, when you give someone the validation string, you must use a method that guarantees its authenticity. For example, you can send people the *key* file as an e-mail attachment or stored on a floppy diskette, and tell them the validation string in person or by telephone. The validation string can only be considered authentic if the person to whom you give the validation string can recognize your voice. If the person cannot recognize your voice, then another method must be used (for example, registered mail, or a meeting in person).

Note: For improved security, it is best to export a new *key* file whenever you want to give it to someone.

When someone gives you a *key* file, ask the person for the associated validation string. Ensure the validation string is authentic as described above. When you import that *key* file into your address book, the validation string is displayed in a dialog. Compare that validation string with the one you were given. If they match, the *key* file is genuine and can be trusted. If they do not match, ask the person to give you a new copy of the *key* file and the new associated validation string.

Address book

An address book contains the Entrust addresses of people in other domains with whom you plan to exchange protected files. The filename of the file that contains your address book comprises your Client username with a *pab* filename suffix (for example, *John Smith.pab*).

Creating and accessing your address book

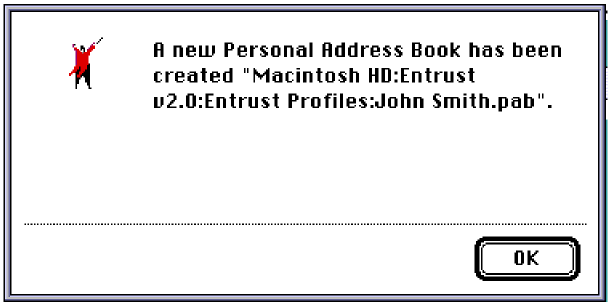
You will need to create an address book if you intend to exchange protected files with people outside of your domain.

To create or access an address book, proceeds as follows:

1. Click the *Address Book* icon on the control palette. Alternatively, you can choose *Address Book...* from the *File* menu.

   Your address book appears immediately if you previously created it.

If this is the first time you access this function or if the Client cannot find your address book, the following dialog appears. The dialog shows the full path to the folder containing your profile (for example, *Macintosh HD: Entrust v2.0:Entrust Profiles:*) and the name of your address book file in that folder (for example, *John Smith.pab*).

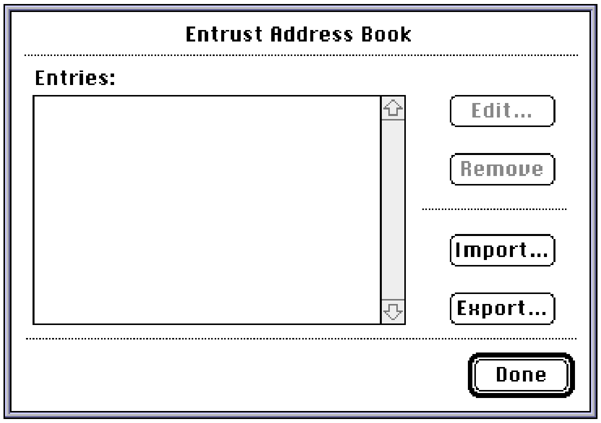


A new Personal Address Book has been created "Macintosh HD:Entrust v2.0:Entrust Profiles:John Smith.pab".

The filename for your address book comprises your Client username followed by a *.pab* filename extension (for example, *John Smith.pab*).

The Client expects to find your address book in the same folder as your profile. If the dialog appears when you have previously created an address book, it is likely that your address book has been moved to a different folder. In such a case, find your previous address book and copy it to the folder containing your profile.

Click *OK* and the *Entrust Address Book* dialog appears.



You can now build your address book by importing the addresses of people with whom you want to exchange protected files.

You can also export your personal Entrust address as explained in “Exporting your personal Entrust address” on page 78.

Building your address book

Building your address book involves importing the addresses of people with whom you plan to exchange protected files. You can add and remove names of people from your address book at any time. Note that when you look at your address book, you will see the names of people who use Entrust outside your domain; you will not see their addresses. The actual address information is stored in your address book and can only be accessed by the Client.

This procedure assumes you already created your address book. If you have not yet accessed your address book, refer to “Creating and accessing your address book” on page 72.

To import names of people to your address book, proceed as follows:

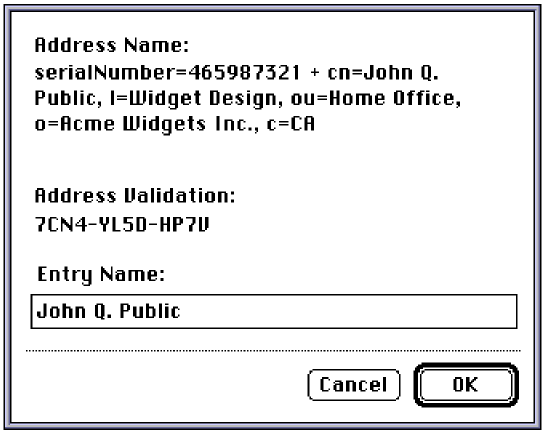
1. From the *Entrust Address Book* dialog, click *Import...*

   A standard file selection dialog appears.

2. From this dialog, locate the *key* file that contains the address you want to add to your address book (for example, *John Public.key*). If necessary, change folder or drive.

3. Once you have found the *key* file, select it and click *Open*.

   A dialog showing the validation string associated with the address you are adding to your address book appears.



Address Name:
serialNumber=465987321 + cn=John Q. Public, l=Widget Design, ou=Home Office, o=Acme Widgets Inc., c=CA

Address Validation:
7CN4-YL5D-HP7V

Entry Name: John Q. Public

4. Check the validation string (for example, 7CN4-YL5D-HP7V) in the dialog. It must match exactly the validation string the person gave you.

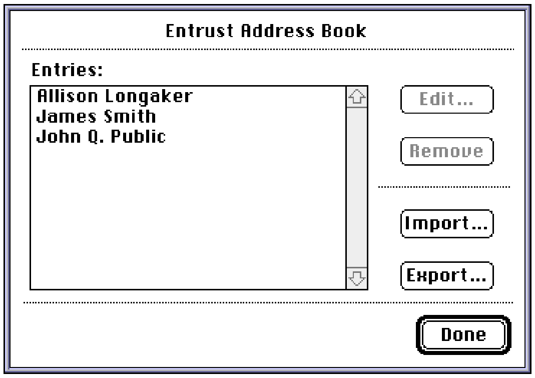
   If the validation string does not match, the *key* file may have been altered, damaged, or maliciously changed since it was created. Ask the person who gave you the *key* file to give you a new *key* file and the associated validation string.

If the validation string matches, continue at step 5.

5. Click OK.

   The *Entrust Address Book* dialog reappears and the name of the person you just added appears in your address book.

6. Repeat the procedure as many times as you have addresses you want to add to your address book.



Allison Longaker
James Smith
John Q. Public

7. Click *Done* once you are finished adding people to your address book.

Now you can encrypt and sign files for anyone listed in your address book.

Whenever you need to exchange protected files with an Entrust user outside your domain, you can retrieve the user's name from your address book when selecting recipients for your encrypted file. For information about selecting people from your address book, refer to "Selecting recipients by name in personal address book" on page 49.

Changing the contents of your address book

You can make the following changes to your address book:

- Remove the names of people from your address book.
- Change the names of people who are already in your address book.
- Re-import the addresses of people who are already in your address book.

Removing names from your address book

To remove the name of a person from your address book, proceed as follows:

1. From the *Entrust Address Book* dialog, select the name you want to remove.

2. Click *Remove* to remove the person.

   You will be prompted for confirmation.

3. Click *Yes* if you want to proceed.

   The *Entrust Address Book* dialog reappears.

4. Click *Done* to leave the dialog.

Changing the names of people who are already in your address book

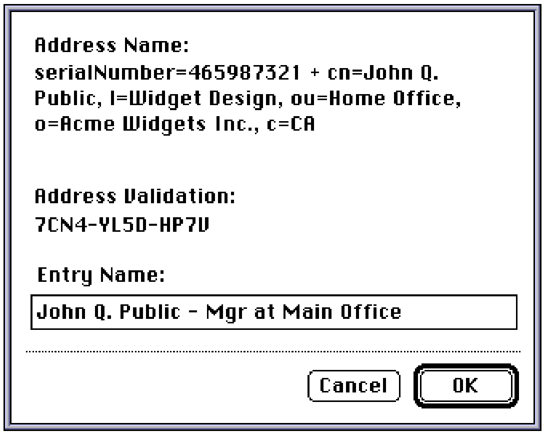
You can change the name of a person who is already listed in your address book. You might do this if you want to add more information to the name (for example, the person's company name). This change has no effect on the person's Entrust address. It only changes the way the person's name appears in your address book.

To change the name of a person who is already listed in your address book, proceed as follows:

1. From the *Entrust Address Book* dialog, select the person whose name you want to change.

2. Click *Edit...*.

   A dialog appears displaying information about the person whose name you are changing. The current name appears in the *Entry Name* field.



Address Name:
serialNumber=465987321 + cn=John Q. Public, l=Widget Design, ou=Home Office, o=Acme Widgets Inc., c=CA

Address Validation:
7CN4-YL5D-HP7V

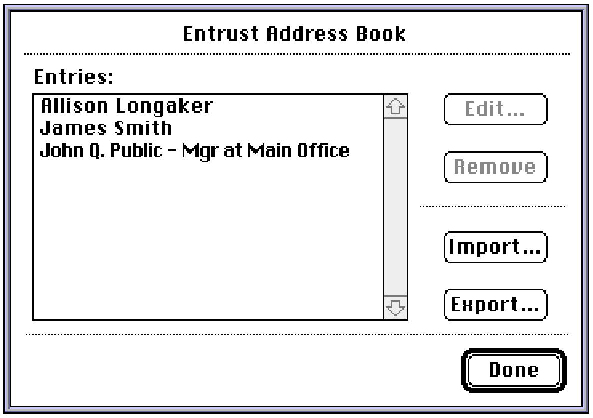
Entry Name:
John Q. Public - Mgr at Main Office

3. Enter a unique name for the person in the *Entry Name* field at the bottom of the dialog.

   This is the name that will appear in your address book.

4. Click *OK*.

The *Entrust Address Book* dialog reappears and the edited version of the name appears in the *Entries* list.



Entrust Address Book

Entries:

Allison Longaker
James Smith
John Q. Public - Mgr at Main Office

Re-importing the addresses of people into your address book

If people whose names already appear in your address book change their Entrust addresses (for example, if they move from one company to another), you will need to delete the old addresses from your address book and re-import each person’s new address.

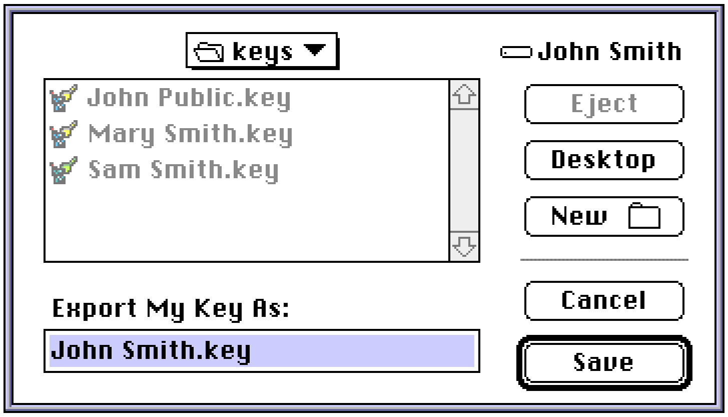
If people whose names already appear in your address book ever recover their Client username, (as explained in “Recovering your Entrust/Client username” on page 96) those people should give you new *key* files (and associated validation strings) which you should import into your address book.

Exporting your personal Entrust address

To allow other people outside your Entrust domain to send protected files to you, you must give them your Entrust address. This address must be placed in a special file called a *key* file as follows:

1. From the *Entrust Address Book* dialog, click *Export...*

   A standard file selection dialog appears displaying the name of a file in the field labeled *Export My Key As*. The default filename comprises your Client username with a *.key* suffix (for example*, John Smith.key*). The dialog also shows the name of the folder in which the file will be stored.

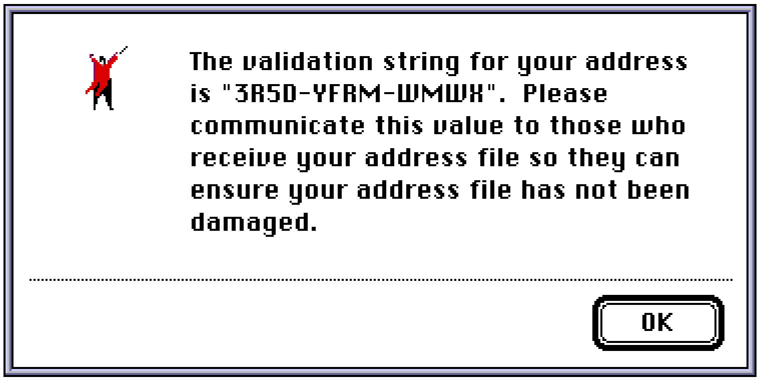


Export My Key As: John Smith.key

2. If you want to use the default filename displayed in the *Export My Key As* field for your *key* file, click *Save*.

   Alternatively, you can enter a different filename. You can also navigate to a different folder in which the file is to be stored or you can create a new folder.

A dialog appears displaying the validation string associated with your address (for example, 3R5D-YFRM-WMWX).



The validation string for your address is "3R5D-YFRM-WMWX". Please communicate this value to those who receive your address file so they can ensure your address file has not been damaged.

3. Click *OK*.

The *Entrust Address Book* dialog reappears.

The *key* file containing your Entrust address is created. You can give this file to Client users in other Entrust domains so they can encrypt files for you. Remember to tell these users the validation string associated with your address. You should give people the *key* file and the validation string separately (unless you give them this information in person). For example, you can send people the *key* file as an e-mail attachment or stored on a floppy diskette, and tell them the validation string in person or by telephone. When you give someone the validation string, you must use a method that guarantees its authenticity. For example, if you tell them the validation string by telephone, the validation string can only be considered authentic if the person to whom you give the validation string can recognize your voice. If the person cannot recognize your voice, then another method must be used (for example, registered mail, or a meeting in person).

Using saved lists of recipients

An Entrust/Client recipient list is a set of recipients and options for encrypting and signing that you select and store under a *recipient list* name. Instead of having to specify each recipient and option every time you want to protect files, you can specify the name of a recipient list. You control who is part of a recipient list and you can create more than one recipient list. For example, you could create one recipient list for each project you work on. Note that a recipient can be a member of more than one recipient list.

For example, you may find that you always use file compression and ASCII encoding when you protect files to be sent to a group of users via e-mail but that you use other options when you frequently protect files for a different group of users. For those two scenarios, you could create two separate recipient lists that would make protecting files for these groups of users very simple.

A recipient list can include recipients who are part of your CA security domain and Entrust users in other domains. To include recipients from other domains, you first need to import their Entrust addresses. See “Exchanging protected files with Entrust users in different domains” on page 71 for more information about including recipients from other domains.

An important feature of recipient lists is that they can be shared with other Client users in your domain. For example, if you and your colleagues use some of the same recipient lists on a regular basis, you can share them instead of maintaining your own copies of the same recipient lists. You can share your own recipient lists by exporting them, or you can share other users’ recipient lists by importing them. Refer to “Sharing recipient lists” on page 87.

The recipient list information that the Client uses is stored in a separate file. The filename is the same as your username. A *.erl* filename extension (for example, *John Smith.erl*) is automatically added to the filename of the recipient list file.

Recipient list management functions are as follows:

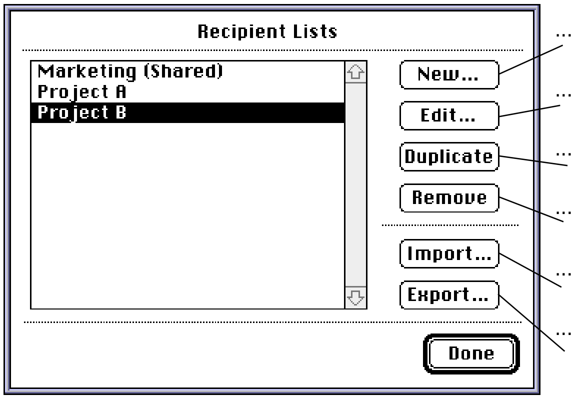
- creating recipient lists
- changing recipient lists
- duplicating recipient lists
- deleting recipient lists
- sharing your recipient lists with other users
- sharing other users’ recipient lists

Accessing recipient list management functions

Proceed as follows to access recipient list management functions:

1. Click the *Recipient Lists* icon on the control palette.

The *Recipient Lists* dialog appears. Note that in this example there are some existing recipient lists.



Click to...

... create a new recipient list.

... edit the selected recipient list.

... duplicate the selected recipient list.

... delete the selected recipient list.

... import a shared recipient list.

... share the selected recipient list.

2. From the *Recipient Lists* dialog you can:

- create new recipient lists (see “Creating a new recipient list” on page 82)
- change existing recipient lists (see “Changing an existing recipient list” on page 84)
- duplicate existing recipient lists
- delete existing recipient lists (see “Deleting an existing recipient list” on page 86)
- share your recipient lists (see “Sharing your recipient lists with other users” on page 87)
- import shared recipient lists (see “Sharing other users’ recipient lists” on page 89)

Creating a new recipient list

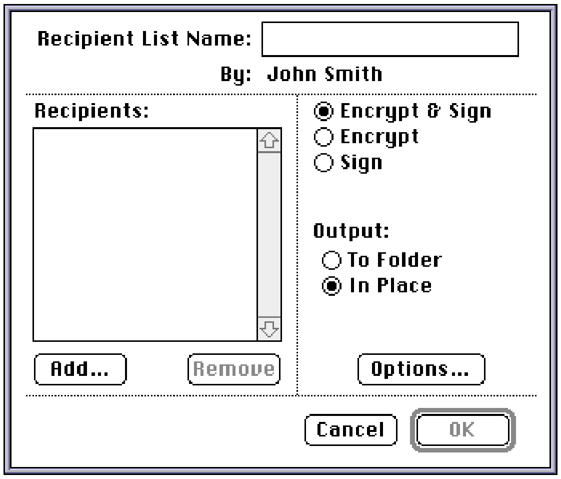
This procedure assumes that the *Recipient Lists* dialog is displayed. If it is not, refer to “Accessing recipient list management functions” on page 81.

> ***Note:*** If you want to create a new recipient list that is based on an existing recipient list, duplicate an existing recipient list and then make changes to the new (duplicate) recipient list. Refer to “Changing an existing recipient list” on page 84 for information about making changes to a recipient list.

To create a new recipient list, proceed as follows:

1. Click *New...* in the *Recipient Lists* dialog.

   The following dialog appears.



Recipient List Name:

By: John Smith

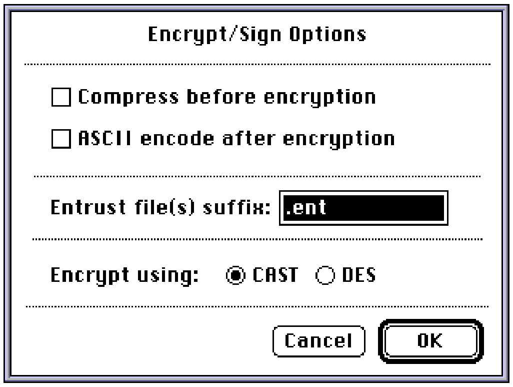
Recipients:

● Encrypt & Sign
○ Encrypt
○ Sign

Output:
○ To Folder
● In Place

2. Enter the name of your new recipient list in the *Recipient List Name* field in the dialog.
3. Select one of the encrypt and sign options. The protection option you choose will be automatically selected whenever you use the recipient list in the *Encrypt & Sign* dialog. For more information about these options, refer to “Selecting encrypting and signing options” on page 58.
4. Notice the *Output* radiobuttons. The *Output* radiobutton you choose will be automatically selected whenever you use the recipient list in the *Encrypt & Sign* dialog. For more information about the *Output* radiobuttons, refer to “Selecting encrypting and signing options” on page 58.
5. Click *Options...* in the dialog.

The *Encrypt/Sign Options* dialog appears.



Encrypt/Sign Options

□ Compress before encryption

□ ASCII encode after encryption

Entrust file(s) suffix: .ent

Encrypt using: ● CAST ○ DES

Encrypt and sign options you can select are as follows:

- Compress before encryption
- ASCII encode after encryption
- Entrust file(s) suffix
- Encrypt using

The options you choose in the *Encrypt/Sign Options* dialog will be automatically selected whenever you use the recipient list in the *Encrypt & Sign* dialog. For more information about the options, refer to “Selecting encrypting and signing options” on page 58.

Click *OK* to leave the *Encrypt/Sign Options* dialog once you have selected the appropriate options for the recipient list.

6. Click *Add…* to specify the recipients to be stored as part of the recipient list.

   The rest of the procedure for adding recipients to a recipient list depends on whether you want to add recipients by

   - searching for names of people (see “Selecting recipients by name” on page 44 for more information)
   - selecting names of people who are members of one of your existing recipient lists (see “Selecting an existing recipient list from the Select Entrust Recipients dialog” on page 55 for more information)
   - selecting names of people whom you previously imported into your address book (see “Selecting recipients by name in personal address book” on page 49 for more information)

   You can add names to the recipient list by combining any of these three methods. You can also delete recipients from a recipient list.

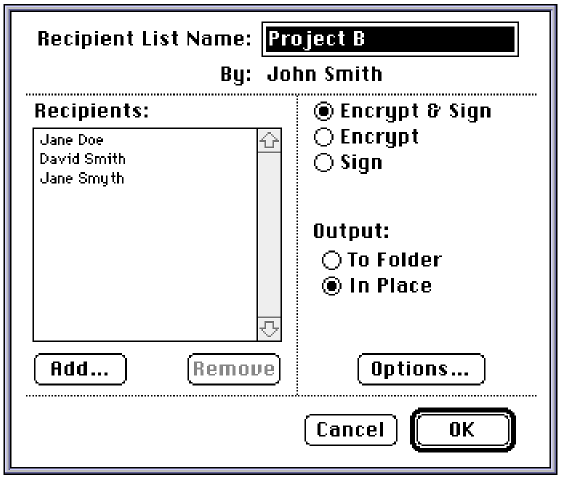
Changing an existing recipient list

This procedure assumes that the *Recipient Lists* dialog is displayed. If it is not, refer to “Accessing recipient list management functions” on page 81.

To change an existing recipient list, proceed as follows:

1. Select the recipient list name from the *Recipient Lists* dialog and click *Edit...* Alternatively, you can double-click the recipient list name.

The following dialog appears. The name of the recipient list you selected appears in the *Recipient List Name* field and the recipients that are currently members of the recipient list appear in the *Recipients* section of the dialog.



Recipient List Name: Project B

By: John Smith

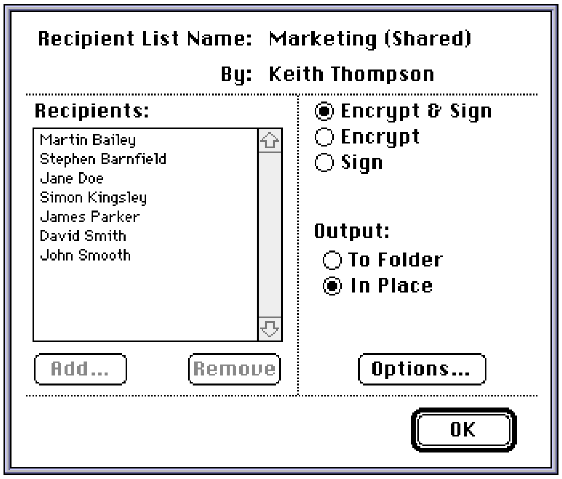
Recipients:

Jane Doe
David Smith
Jane Smyth

● Encrypt & Sign
○ Encrypt
○ Sign

Output:
○ To Folder
● In Place

If the *Recipient List Name* shows the name of a shared recipient list (indicated by *(Shared)* following the recipient list name), you will not be able to modify the shared recipient list. Shared recipient lists cannot be modified directly. Only the originators of shared recipient lists can make changes to shared recipient lists and they can only change the original recipient lists; they cannot edit the shared version of the recipient lists. If a shared recipient list appears in the dialog, the *Add…* and *Remove* buttons are disabled. Refer to “Sharing recipient lists” on page 87 for information about shared recipient lists.



Recipient List Name: Marketing (Shared)

By: Keith Thompson

Recipients:

Martin Bailey
Stephen Barnfield
Jane Doe
Simon Kingsley
James Parker
David Smith
John Smooth

● Encrypt & Sign
○ Encrypt
○ Sign

Output:
○ To Folder
● In Place

2. Notice the *By* field.

   The *By* field shows the name of the person who created the recipient list. This field will show your name, except when you are looking at a shared recipient list created by another person.

3. Select options to be stored with your recipient list. Refer to step 3. in “Creating a new recipient list” on page 82 for information about selecting options in a recipient list.

The rest of the procedure for changing an existing recipient list depends on whether you want to add recipients by

- searching for names of people (see “Selecting recipients by name” on page 44 for more information)
- selecting names of people who are members of one of your existing recipient lists (see “Selecting an existing recipient list from the Select Entrust Recipients dialog” on page 55 for more information)
- selecting names of people whom you previously imported into your address book (see “Selecting recipients by name in personal address book” on page 49 for more information)

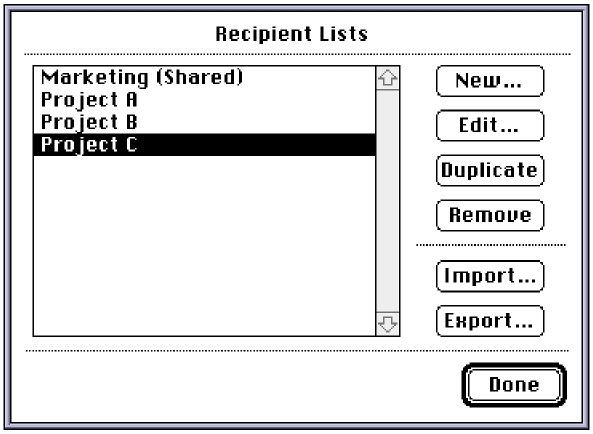
You can add names to the recipient list by combining any of these three methods. You can also delete recipients from a recipient list.

Deleting an existing recipient list

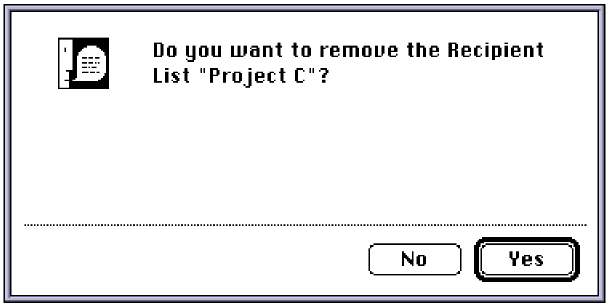
This section assumes the *Recipient List* dialog is displayed. If it is not, refer to “Accessing recipient list management functions” on page 81.

To delete an existing recipient list, proceed as follows:

1. Select the recipient list name you want to delete from the *Recipient List* dialog and click *Remove...*



A confirmation dialog similar to the following appears.


Do you want to remove the Recipient List "Project C"?

2. Click *Yes*.

   The *Recipient Lists* dialog reappears.

Your recipient list is deleted.

Sharing recipient lists

An important feature of recipient lists is that you can share them with other Client users in your CA security domain. For example, if you and your colleagues use some of the same recipient lists on a regular basis, you can share them instead of maintaining your own copies of the same recipient lists.

You can share some of your own recipient lists with others; similarly, you can use a recipient list that was created by someone else.

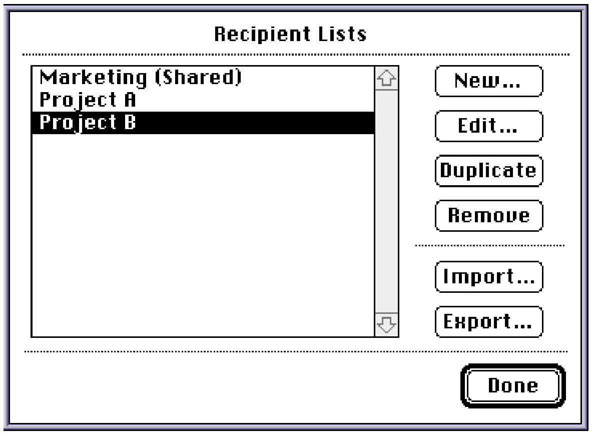
Sharing your recipient lists with other users

This section assumes the *Recipient List* dialog is displayed. If it is not, refer to "Accessing recipient list management functions" on page 81.

To share your recipient lists, proceed as follows:

1. Select the recipient list name you want to share from the *Recipient List* dialog and click *Export...*

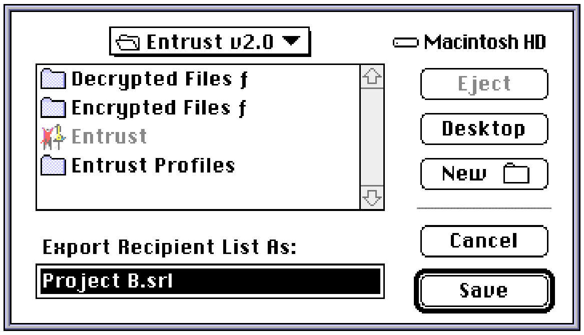
   Note: If the recipient list you select contains recipients from your personal address book, these recipients will be rejected when people try to share the recipient list (unless those people have also imported the Entrust addresses of those recipients into their own personal address books).



Recipient Lists

Marketing (Shared)
Project A
Project B

The following dialog appears.



Export Recipient List As:

Project B.srl

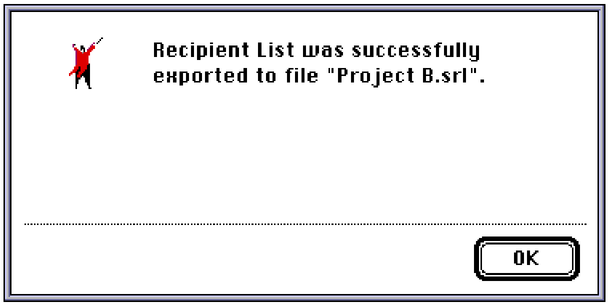
2. In the *Export Recipient List As* field, enter a filename for the file in which you want to store your shared recipient list. Notice that the default filename extension is automatically *.srl*. This extension is mandatory and cannot be changed.

   If you plan to share your recipient list with others who use the Client on platforms other than the Macintosh, ensure you choose a filename that can be accessed on the other platforms (for example, *projB.srl*). The name of the shared recipient list is stored as part of the list; therefore, the name of the file storing the shared recipient list can be changed without affecting the name of the recipient list itself.

3. Choose a folder in which you want to store your shared recipient list file.

4. Click *OK* in the dialog.

   A message similar to the following appears.



Recipient List was successfully exported to file "Project B.srl".

5. Click *OK*.

   The *Recipient Lists* dialog reappears.

Your recipient list has been exported. Ensure this file is stored in a directory to which others have access so they can use this recipient list when selecting recipients or when creating or editing other recipient lists.

ATTENTION
Shared recipient lists cannot be modified by anyone including the originator. Therefore you should keep a copy of the recipient list that you exported in case you need to need to make changes later. If you make changes to the recipient list, you will need to re-export the recipient list.

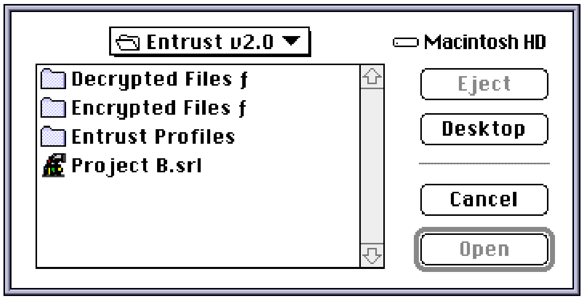
Sharing other users' recipient lists

This section assumes the *Recipient Lists* dialog is displayed. If it is not, refer to "Accessing recipient list management functions" on page 81.

To access recipient lists that were created by other users and that have been designated as shared recipient lists, proceed as follows:

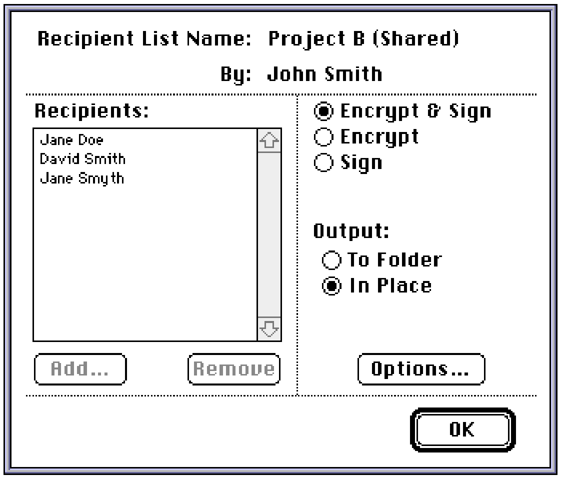
1. Click *Import...* in the *Recipient Lists* dialog.

   The following dialog appears.



2. From this dialog, locate and select the *srl* file that contains the recipient list you want to use (for example, *Project B.srl*). If necessary, change folder or drive.
3. Click *Open* in the dialog.

The following dialog appears.



Recipient List Name: Project B (Shared)

By: John Smith

Recipients:

Jane Doe
David Smith
Jane Smyth

● Encrypt & Sign
○ Encrypt
○ Sign

Output:

○ To Folder
● In Place

4. Notice the *By* field.

   The *By* field shows the name of the person who created the shared recipient list.

5. Review the recipient list and decide if you want to keep it. Click the *Options…* button to view the other options defined by the creator of the recipient list. You cannot make changes to a shared recipient list.

   If you decide you do not want to keep the shared recipient list, you can delete it using the *Remove* button in the *Recipient Lists* dialog.

6. Click *OK* in the dialog.

   The *Recipient Lists* dialog reappears.

You can use a shared recipient list when selecting recipients or when creating or editing other recipient lists. Notice that the recipient lists you imported have the word *Shared* within parentheses in the *Recipient Lists* dialog. When you select a shared recipient list, the *Edit…* button in the *Recipient Lists* dialog changes to *View…* because shared recipient lists cannot be modified.

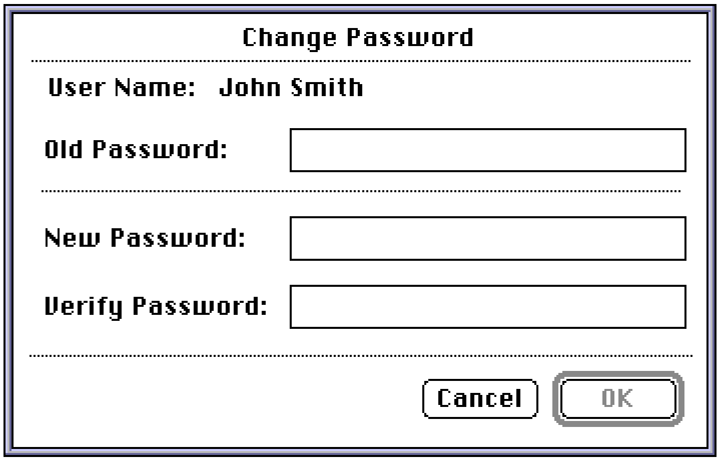
If the originator modifies and re-exports a shared recipient list that you have imported, you will be notified automatically that the recipient list has changed the next time you access it.

Changing your Entrust/Client password

To change your password, proceed as follows:

1. Choose *Change Password...* from the *User* menu.

   The *Change Password* dialog appears.



Change Password

User Name: John Smith

Old Password:

New Password:

Verify Password:

2. Enter your current Client password in the *Old Password* field.
3. Tab to the *New Password* field and enter a password.

   Your Client password must

   - be at least eight characters long
   - contain at least one upper case letter
   - contain at least one lower case letter
   - not contain many occurrences of the same character
   - not be the same as your Client username
   - not contain a substring of your Client username

   The password is case-sensitive. When entering a password, avoid using a common or proper noun. Try to invent a word and include special characters for good measure. Examples of special characters are: $, +, =, !, ~, ^ and &. A good password is one that is difficult to guess and easy to remember (for example, H2OPlsNow! (water please, now!)). For more information about passwords, refer to “Appendix C: Entrust password security.”

4. Tab to the *Verify Password* field and enter the same password again.

The reason you need to enter your new password twice is to ensure that you typed exactly what you meant to type. Entrust checks to ensure that you entered your new password exactly the same way both times.

If you write down your password, store it in a locked place to which only you have access.

5. Click *OK*.

   Your password is changed.

Creating additional Entrust/Client users

There may be occasions when more than one user needs to use the Client on a particular computer. Client users can log on to the Client on any machine as long they make their profiles available (for example, on an inserted floppy diskette). However, if the person has not yet created a Client username, a username must first be created.

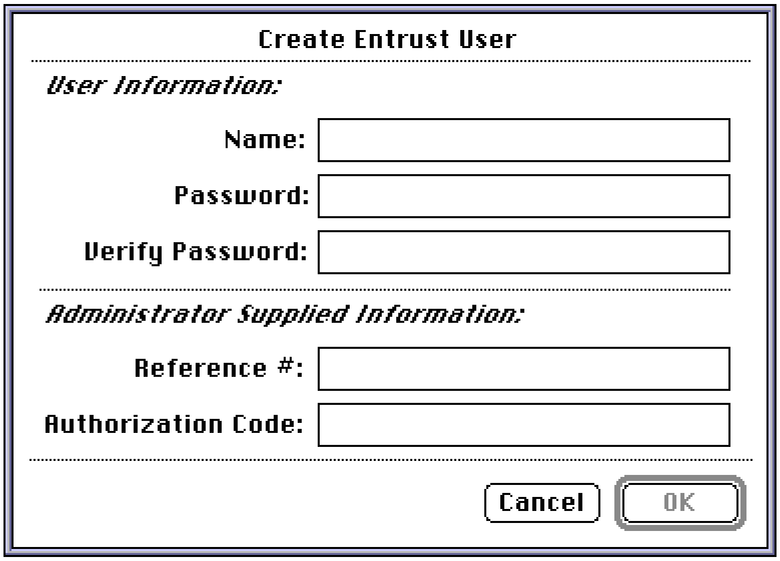
To create a Client username, you will need a reference number and an authorization code. If you do not have this information already, contact your Entrust Administrator to obtain it.

> ***Note:*** The reference number and authorization code can only be used once to create one user after which they become invalid and cannot be used again.

To create a Client username:

1. Select *Create User...* from the *User* menu.

The *Create Entrust User* dialog appears.



Create Entrust User

User Information:

Name:

Password:

Verify Password:

Administrator Supplied Information:

Reference #:

Authorization Code:

2. Enter your name in the *Name* field.

You can choose any you like (for example, *John Smith*).

3. Tab to the *Password* field and enter a password.

   Your Client password must

   - be at least eight characters long
   - contain at least one upper case letter
   - contain at least one lower case letter
   - not contain many occurrences of the same character
   - not be the same as your Client username
   - not contain a substring of your Client username

   The password is case-sensitive. When entering a password, avoid using a common or proper noun. Try to invent a word and include special characters for good measure. Examples of special characters are: $, +, =, !, ~, ^ and &. A good password is one that is difficult to guess and easy to remember (for example, H2OPlsNow! (water please, now!)). For more information about passwords, refer to “Appendix C: Entrust password security.”

4. Tab to the *Verify Password* field and enter the same password again.

   The reason you need to enter your new password twice is to ensure that you typed exactly what you meant to type. The Client checks to ensure that you entered your new password exactly the same way both times.

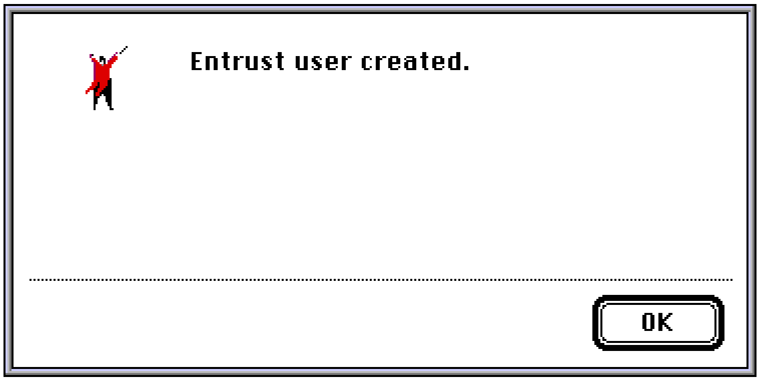
   If you write down your password, store it in a locked place to which only you have access.

5. Tab to the *Reference #* field and enter the reference number you obtained from your Administrator (for example, 22172260).

6. Tab to the *Authorization Code* field and enter the code you obtained from your Administrator (for example, 7GNP-QI36-HAWG).

7. Click *OK* in the *Create Entrust User* dialog.

After a short period of time, a message appears confirming that a new Entrust user was created.



Entrust user created.

8. Click *OK*.

The Entrust control palette appears with the name of the new user displayed.

You can now encrypt, decrypt, sign, and verify files. You can also create your address book, create groups of recipients, specify preferences, and change your password.

If the Client was unable to create a new user, try supplying the information again. Ensure that you enter the reference number and the authorization code in exactly the same form as you received them from your Entrust Administrator. If you still cannot create a Client username, contact your Administrator.

Recovering your Entrust/Client username

You will need to recover your username if you

- forget your password
- lose your Entrust profile or it becomes corrupt

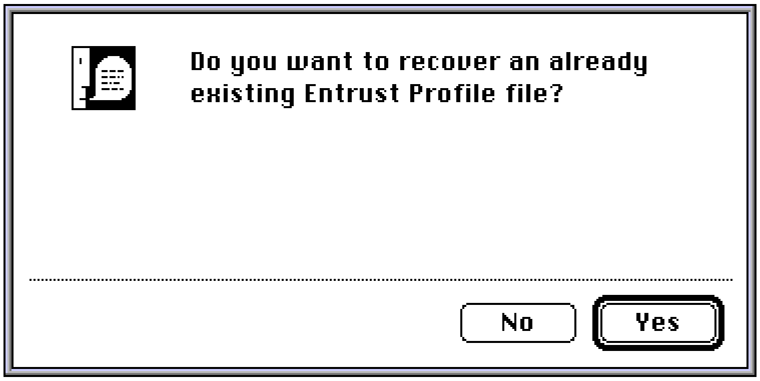
Before you can recover your username, you need to contact your Administrator to obtain a new reference number and authorization code. Once you have this information, you can recover your username by following these steps:

1. Start up Entrust as you usually do.

The Entrust control palette appears.

2. Choose *Recover Use*r... from the *File* menu.

The following dialog appears.



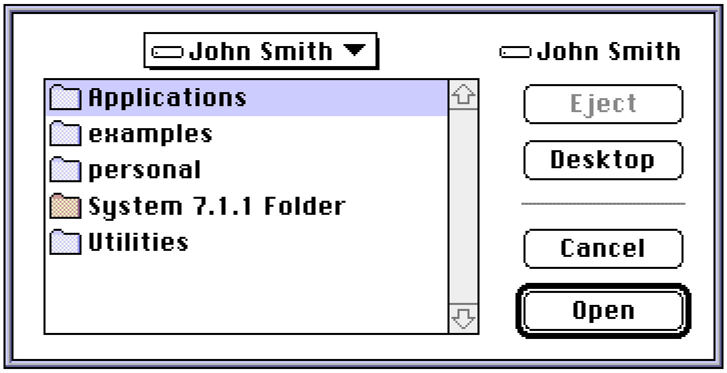
Do you want to recover an already existing Entrust Profile file?

3. If you still have a copy of your profile, click *Yes*.

This case typically applies if you are recovering your Client username because you forgot your Client password.

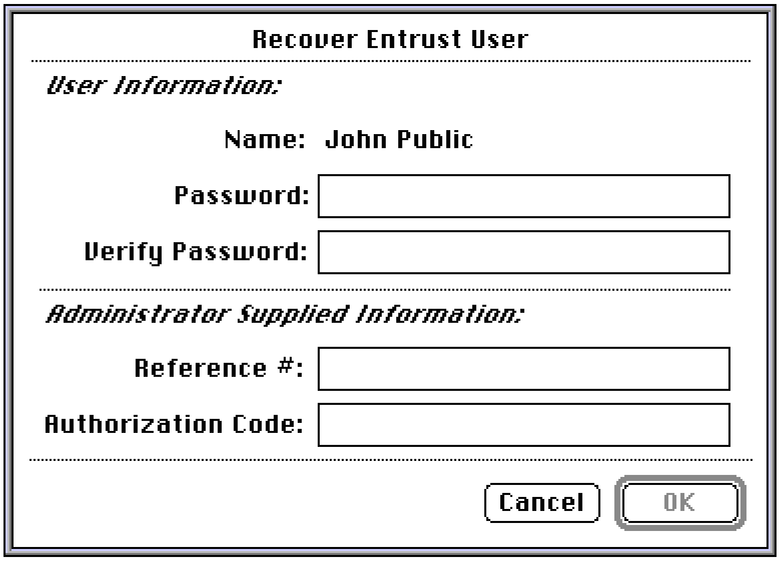
If you no longer have a copy of your profile, click *No* and skip to step 5. Note that any groups you may have previously created cannot be recovered because group information is stored in your Client profile. This case applies if you lost your profile or it has become corrupt.

If you clicked *Yes*, a standard file selection dialog appears.



4. From the file selection dialog, locate your Client profile, select it and click *Open*.

   The *Recover Entrust User* dialog appears.



Recover Entrust User

User Information:

Name: John Public

Password:

Verify Password:

Administrator Supplied Information:

Reference #:

Authorization Code:

5. Enter your name in the *Name* field.

   You can choose any you like (for example, *John Smith*).

   Note: If you are reusing an existing profile, the *Name* field is automatically filled in.

6. Tab to the *Password* field and enter a password.

Your Client password must

- be at least eight characters long
- contain at least one upper case letter
- contain at least one lower case letter
- not contain many occurrences of the same character
- not be the same as your Client username
- not contain a substring of your Client username

The password is case-sensitive. When entering a password, avoid using a common or proper noun. Try to invent a word and include special characters for good measure. Examples of special characters are: $, +, =, !, ~, ^ and &. A good password is one that is difficult to guess and easy to remember (for example, H2OPlsNow! (water please, now!)). For more information about passwords, refer to “Appendix C: Entrust password security.”

7. Tab to the *Verify Password* field and enter the same password again.

The reason you need to enter your new password twice is to ensure that you typed exactly what you meant to type. The Client checks to ensure that you entered your new password exactly the same way both times.

If you write down your password, store it in a locked place to which only you have access.

8. Tab to the *Reference #* field and enter the reference number you obtained from your Administrator (for example, 22172260).

9. Tab to the *Authorization Code* field and enter the code you obtained from your Administrator (for example, 7GNP-QI36-HAWG).

10. Click *OK*.

After a short period of time, a message appears confirming that your username has been recovered.

Your username has been recovered. You can resume use of the Client.

If the Client was unable to recover your Client username, try supplying the information again. Ensure that you enter the reference number and the authorization code in exactly the same form as you received them from your Entrust Administrator. If you still cannot recover your Client username, contact your Administrator.

Setting Entrust/Client preferences

When you first install the Client, various operations, options, and text fields have default values. You can change these values to suit your preferences. These values remain in effect until you change them again.

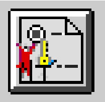
You can set defaults for the following groups of options:

- Encrypt/Sign options
- Other options

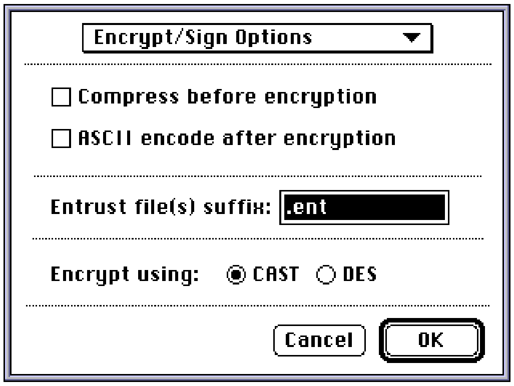
> ***Note:*** You can also change the *Encrypt/Sign* options by clicking *Options...* in the *Encrypt & Sign* dialog.

To set defaults for various operations, options, and text fields, proceed as follows:

1. Select the *Preferences* icon in the control palette or choose *Preferences...* from the *File* menu.



   The following dialog appears.



Encrypt/Sign Options

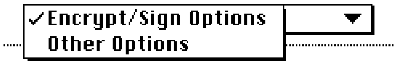
□ Compress before encryption

□ ASCII encode after encryption

Entrust file(s) suffix: .ent

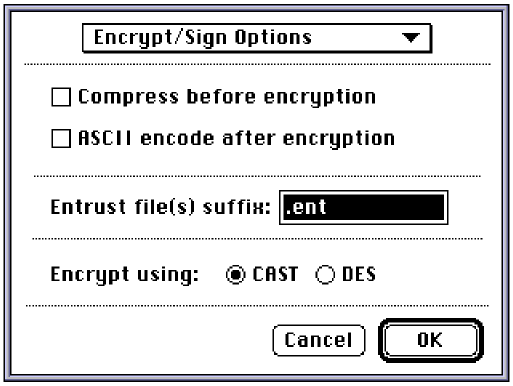
Encrypt using: ● CAST ○ DES

2. Select the options for which you want to specify defaults from the pop-up menu at the top of the dialog.



Encrypting and signing options

Select *Encrypt/Sign Options* from the pop-up menu at the top of the dialog to set the defaults for encryption and digital signature options. The following are the options for which you can specify defaults:



☐ Compress before encryption

☐ ASCII encode after encryption

Entrust file(s) suffix: .ent

Encrypt using: ● CAST ○ DES

Compress before encryption

Select *Compress before encryption* to compress the files before they are protected. It is necessary to compress files before they are encrypted because it is impossible to compress an encrypted file. By definition, an encrypted file is completely random, making compression impossible. The amount of compression depends on the type of file. Word processing files can generally be compressed to less than half their original size. Graphics files can often be compressed even more than word processing files.

ASCII encode after encryption

Select this option to force the Client to use an ASCII file format when encrypting files. If you do not select this option, the Client will use a binary format. The advantage of using the binary format is that the resulting size of the protected file will be about 30% smaller than if you use the ASCII file format, and it will take a shorter time to process files. However, the ASCII option is mandatory if you plan to transfer the protected file using an electronic file transfer mechanism like ASCII-FTP or certain electronic mail systems that can only handle ASCII file formats.

Entrust file(s) suffix

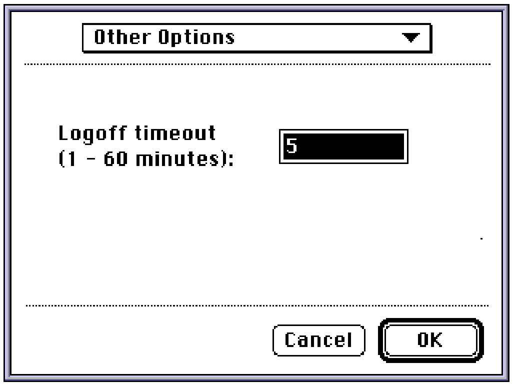
Once your file is protected, its filename will receive the suffix specified in the *Entrust file(s) suffix* field. The default suffix is *ent*. You can change the output file suffix by entering a different one. It is recommended that you use the default *ent* suffix to achieve consistency among Client users across all supported platforms. Using the default also makes it easier to find protected files. When you protect a file, the Client first makes a copy of the file which it then encrypts and/or signs. For example, if you encrypt and sign a file called *report7.doc*, the Client encrypts and signs a copy of the file which is called *report7.doc.ent*. You can select the *Delete source file* option in the *Encrypt & Sign* dialog to automatically delete the original file after it is protected.

Encryption method

CAST and DES are two encryption methods available to the Client to protect your files. Typically, the decision on which to use is a policy adopted by your organization with guidance from your Administrator.

Other options

Select *Other Options* from the pop-up menu at the top of the preferences dialog to set the default for this option.



Logoff timeout (1 - 60 minutes): 5

The Client automatically logs you out a preset number of minutes after you last used the Client. You can choose to set this number to between 1 and 60 minutes. Enter a value that suits your needs. This option reduces the risk of someone signing files with your digital signature or decrypting your files while you are temporarily away from your computer.

Using Entrust/Client on different computers

You can use the Client on any computer in your organization that has the Client installed (for example, Macintosh computers, UNIX workstations, and PCs running Microsoft Windows). All you need to do is make a copy of your Client profile (for example, *John Smith)* and transfer it to the computer you want to use by means of a floppy diskette or some electronic file transfer mechanism. You should also transfer a copy of your recipient lists file (for example, *John Smith.erl*) to the same directory as your profile. If you intend to use your address book to protect files for users outside your organization, you must also transfer the file containing your address book (for example, *John Smith.pab*) to the same directory as your profile.

ATTENTION

Even though your personal information stored in your profile is encrypted, you should still take precautions to ensure nobody obtains a copy of your profile. You need to be particularly careful when transferring your profile across various computers.

You may need to rename files before you move them between different platforms. The filenames must conform to the filename conventions used by the new platform. For example, if you move your profile from a Macintosh to another platform, you will need to rename your profile from *John Smith* to *johnsmit.epf*. If you also move your address book, rename it from *John Smith.pab* to *johnsmit.pab*. Similarly, you should rename your recipient lists file from *John Smith.erl* to *johnsmit.erl*.

When you start the Client on the new platform, use the *Find Profile...* button on the *Entrust Log On* dialog to locate your Client profile on that computer and select your profile.

Once you are logged on, you should check the fields that specify the paths to the folders in which protected and decrypted files are written. Ensure that these folders meet your needs.

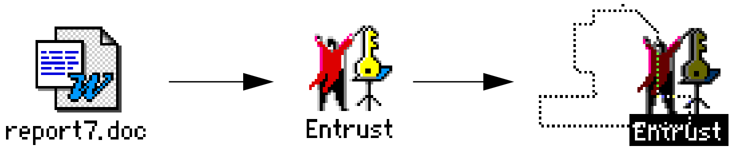
ATTENTION

For increased security, your Entrust information, which is stored in your profile, is automatically updated from time to time. Therefore, you should only keep one copy of your profile. When you need to use a different computer, transfer your profile and delete it from the previous computer. Remember to transfer a new copy of your Client profile back to your other computers if you make changes such as your Client password. This way, your profile will always contain the most current Entrust information. Transfer the updated copy of your address book file to your other computers if you make changes to your address book. Similarly, transfer an updated copy of your recipient lists file (*.erl* filename suffix) if you make changes to any recipient list information.

Starting Entrust/Client

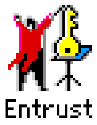
There are several ways to start the Client:

- Drag one or more files (or folders) to Entrust. Refer to “Dragging and dropping files” on page 26 for information about dragging and dropping files.

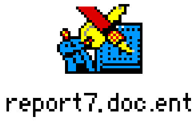


Note: You may find it convenient to store an alias of the *Entrust* icon on the desktop in the Finder to facilitate dragging and dropping files.

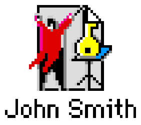
- Double-click the *Entrust* icon.



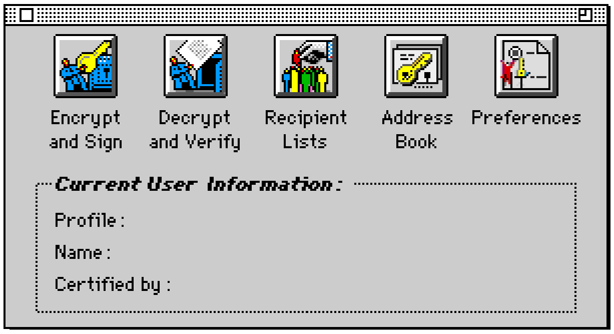
- Double-click a protected file.



- Double-click your *Entrust/Client* profile.



If you double-click the *Entrust* icon, the Client menu bar appears at the top of your screen and the Entrust control palette appears on the desktop. If the control palette does not appear, you can make it visible by selecting *Control Palette...* from the *File* menu. Note that no information appears in the *Current User Information* area of the Entrust control palette until you log on to the Client.



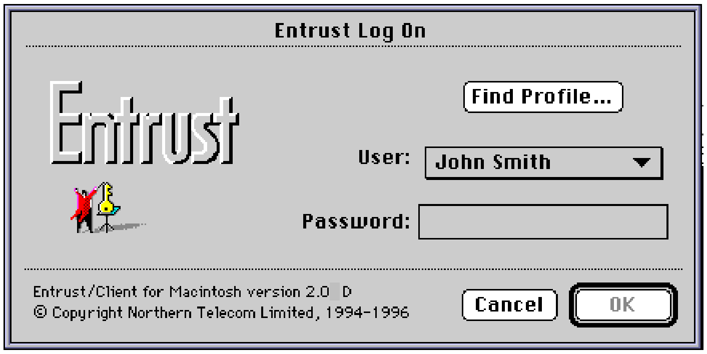
Current User Information :

Profile :

Name :

Certified by :

If you start up the Client using the other methods, the Entrust control palette appears on the desktop with the *Entrust Log On* dialog laid on top of it. You are now ready to log on and start using the Client. Refer to “Logging on to Entrust/Client” on page 107.

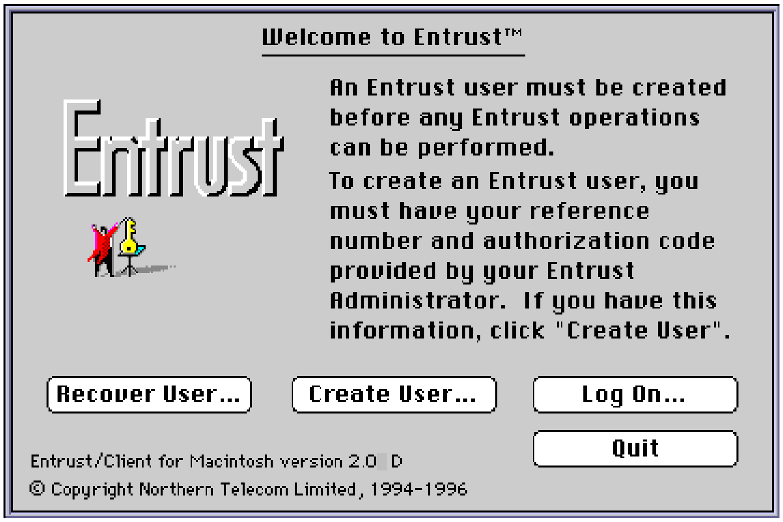


User: John Smith

Password:

Entrust/Client for Macintosh version 2.0 D
© Copyright Northern Telecom Limited, 1994-1996

If the *Welcome to Entrust* dialog appears instead of the *Entrust Log On* dialog, you probably have not yet created your Client username. Click *Create User...* and skip to step 2. in “Creating additional Entrust/Client users” on page 93.



Welcome to Entrust™

An Entrust user must be created before any Entrust operations can be performed.

To create an Entrust user, you must have your reference number and authorization code provided by your Entrust Administrator. If you have this information, click "Create User".

Entrust/Client for Macintosh version 2.0 D

© Copyright Northern Telecom Limited, 1994-1996

Logging on to Entrust/Client

Logging on to the Client is different from starting the Client. Starting the Client involves invoking the application. You cannot use the Client until you log on. The purpose of logging on is to authenticate yourself to Entrust through the use of a password.

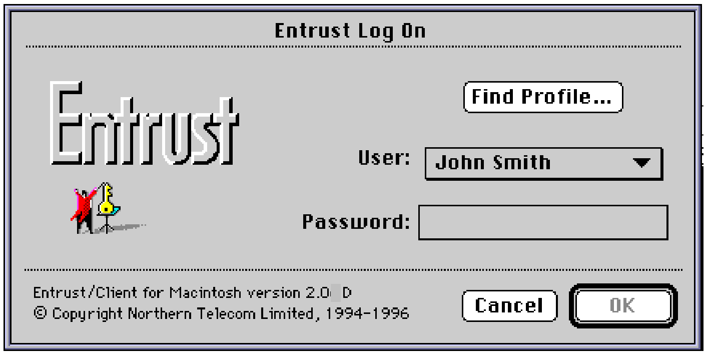
Since Entrust has a safety feature that logs you off a preset number of minutes after you last used the Client, it is possible that you were automatically logged off. To change the preset number of minutes before being automatically logged off, refer to “Other options” on page 101. If you attempt to use the Client while you are logged off, you will automatically be prompted to log on.

To log on to the Client, proceed as follows:

1. Select any Client function and you will be prompted to log on to the Client if you are not already logged on.

Alternatively you can choose *Log On...* from the *User* menu.

The *Entrust Log On* dialog appears.



User: John Smith

Entrust/Client for Macintosh version 2.0 D
© Copyright Northern Telecom Limited, 1994-1996

2. Verify that your username appears in the *User* field (for example, *John Smith*).

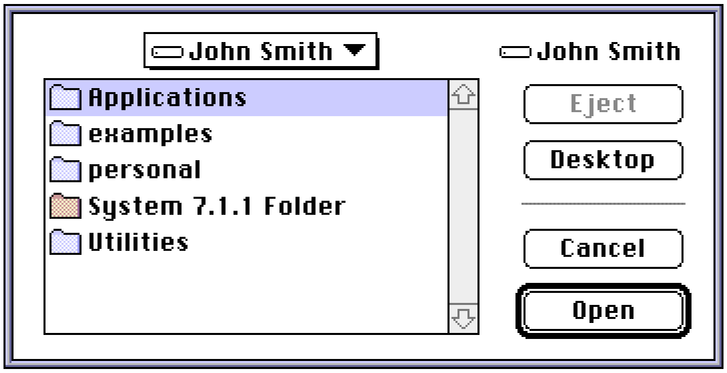
If your username does appear, skip to step 3.

If your username does not appear in the *User* field, click the current username (in this case, *John Smith*) and select your username from the pop-up menu in the *User* field.

If your username is not in the pop-up menu, you will need to locate your Client profile. To locate your profile, proceed as follows:

a. Click *Find Profile...* in the *Entrust Log On* dialog.

A standard file selection dialog appears.



b. From the file selection dialog, locate your Client profile (for example, *John Smith).* If necessary, change folder or drive.

c. Select your profile once you have found it.

d. Click *Open* in the file selection dialog.

The *Entrust Log On* dialog reappears and your username appears in the *Use*r field.

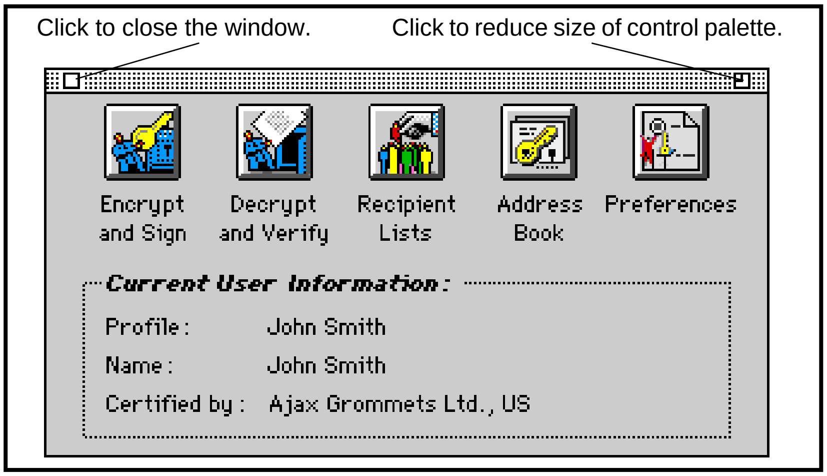
If you cannot locate your profile, contact your Entrust Administrator.

3. Enter your password in the *Entrust Log On* dialog.

4. Click *OK*.

The Client menu bar appears at the top of your screen and the Entrust control palette appears on the desktop. See Figures 6 and 7 on page 109.

Figure 6 Entrust control palette (full size)



Click to close the window.

Click to reduce size of control palette.

Current User Information:

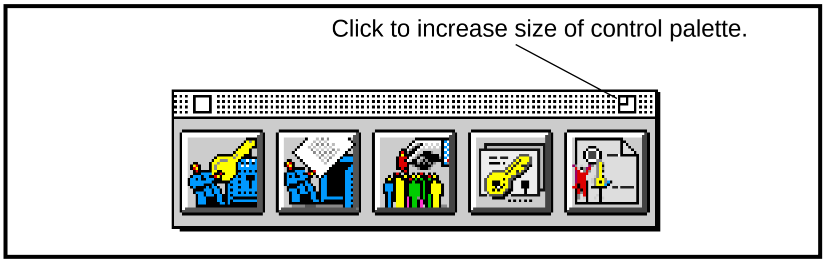
Profile: John Smith

Name: John Smith

Certified by: Ajax Grommets Ltd., US

You can close the control palette by clicking the top-left corner. You can change the size of the control palette by clicking the top-right corner.

Figure 7 Entrust control palette (reduced size)



Click to increase size of control palette.

If the control palette does not appear, you can make it visible by selecting *Control Palette...* from the *File* menu.

Logging off from Entrust/Client

You may choose to log off if you need to step away from your computer and want to ensure that no one can encrypt, decrypt, sign, and verify your files while you are away.

Logging off does not close the Client; it simply prevents anyone from using your Client username without your authorization.

There is also a log-off time-out that automatically logs you off after a preset number of minutes since you last used the Client. You can set the number of minutes in the preferences dialog. To access the preferences dialog, choose *Preferences*... from the *File* menu or click the *Preference*s icon on the control palette.

To log off from the Client, choose *Log Off* from the *User* menu.

Quitting Entrust/Client

To quit your Client session, choose *Quit* from the *File* menu.

Hints

Forgotten password and lost or damaged Entrust profile

If you forget your Client password, or if your Client profile becomes lost or damaged and you do not have a backup, you will have recover your Client username. Ask your Administrator for help.

Using Entrust/Client in different time zones

If you ever change the current time on your computer (for example, because you brought your laptop computer with you to a different location) you should also change the time zone setting that corresponds to your new location. The time on the computer you use to run Entrust/Client must be within two hours of the current time on the clock on which its corresponding Entrust/Manager is running. (Entrust/Manager is the Entrust component that manages all Entrust addresses within your CA security domain.) If your time zone setting does not correspond to your current location, the time zone setting may be sufficiently different to cause a difference in time greater than two hours.

To change the time zone, open the *Map* control panel and enter the name of the city in which your computer is currently being used and click *Find*. If your current city cannot be found, enter the name of the nearest major city that happens to be in the same time zone as your current location. Once you have found city a in your current time zone, click *Set*. The *Map* control panel will automatically set the correct time zone for your current location.

If the time zone setting or the time is incorrectly set on your computer, you may receive a message similar to one of the following when you try to log on to the Client:

```
Could not retrieve up to date certificate revocation list.
```

or

```
The Entrust/Manager time and the time on this machine differ
significantly. Please set the time on your machine correctly
and then try again. Contact your Entrust/Administrator if you
continue to experience difficulty.
```

If you do not change the time on your computer when you move across time zones, you do not need to change time zone setting.

Intended recipient cannot decrypt my files

Problem

A recipient cannot decrypt a protected file that came from you.

Solution

First, try to decrypt the file yourself as a test. If you are able to decrypt the file, it is possible the protected file was damaged in transit. Give the recipient a new copy of the protected file.

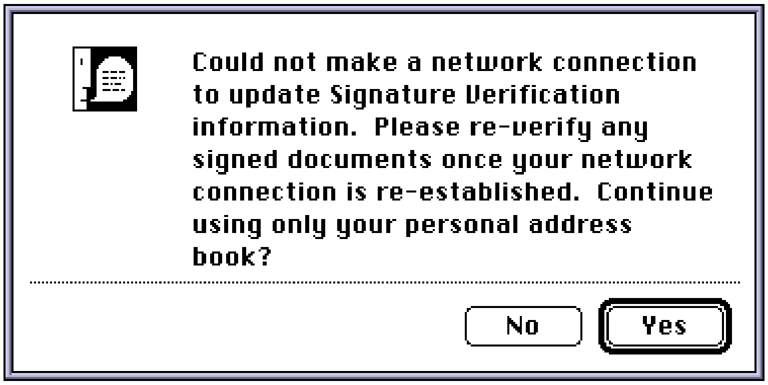
If the person still cannot decrypt the file, check the mechanism you used to give the recipient the protected file. If the file transfer mechanism requires ASCII formatted files, ensure that you used the ASCII option when you encrypted and signed the file.

If the recipient is in a domain that is different from yours, ask the person to give you a new *key* file and import it again into your address book. Then encrypt the file again and give a new copy to your recipient.

If the recipient still cannot decrypt the file, contact your Administrator.

Cannot update your Entrust signature verification information

If the following dialog appears when you log on to Entrust/Client, it is likely that you do not have a network connection. There are many possible causes for loss of network connection. The most common cause is that you are working from a computer that is not connected to the network (for example, you may be working from home). If you are working from a computer that is supposed to be connected to the network, contact your Entrust Administrator for help.

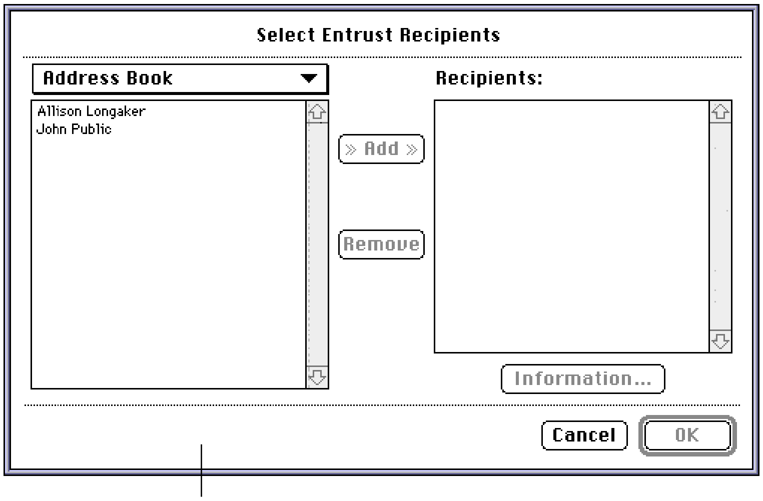


Could not make a network connection to update Signature Verification information. Please re-verify any signed documents once your network connection is re-established. Continue using only your personal address book?

If you choose to continue, you will still be able to use the Client to decrypt files. You will also be able to encrypt and sign files for people listed in your address book. However, you will not be able to create new usernames, recover a username or encrypt files for people who are not listed in your address book.

Although the Client will allow you to verify signatures, you should not necessarily trust the authenticity of the signatures. The reason you should not trust the authenticity of the signatures is that the Client cannot update your Entrust signature verification information. Without access to this information, the Client cannot verify the validity of the signature that was used to sign the file. Once your network connection has been established again, ensure that you reverify every signature that you verified while the Client was not connected to the network.

Search information is unavailable



The search field(s) normally appear in this area.

Problem

The search information field(s) are unavailable in the *Select Entrust Recipients* dialog.

In this situation, you will only be able to encrypt files for people listed in your address book and for people who are members of recipient lists to which you still have access.

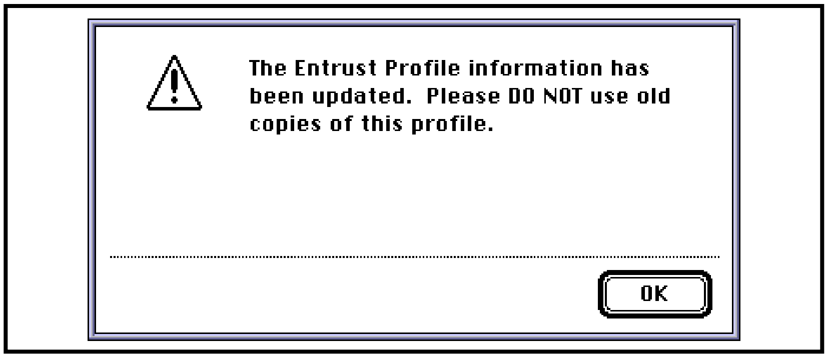
Reason

The probable reason is that you do not have a network connection. For more information about this situation, refer to “Cannot update your Entrust signature verification information” on page 113.

Logging on to the Client after your personal Entrust information has been changed

Problem

The following message appears after to log on to the Client.



The Entrust Profile information has been updated. Please DO NOT use old copies of this profile.

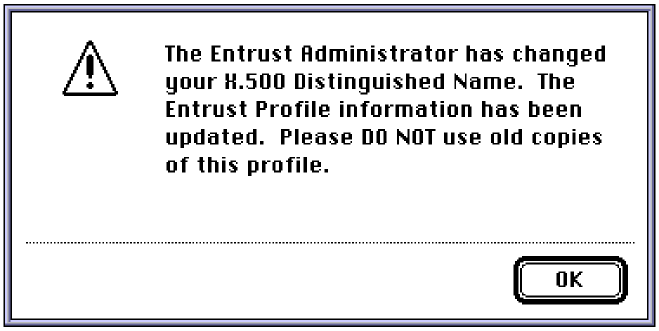
Reason

This message appears because some of your personal Entrust information has been automatically updated. This information is stored in your Client profile. Therefore, if you already made copies of your profile, as described in “Using Entrust/Client on different computers” on page 102, you should replace those outdated copies as soon as possible.

Logging on to the Client after your name has been changed

Problem

The following message appears when you attempt to log on to the Client.



The Entrust Administrator has changed your X.500 Distinguished Name. The Entrust Profile information has been updated. Please DO NOT use old copies of this profile.

Reason

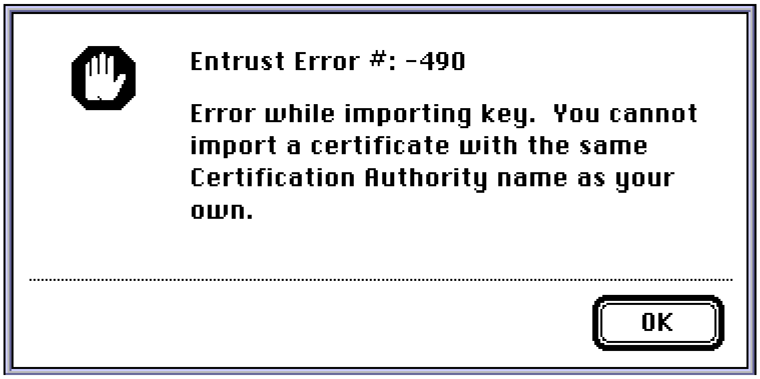
This message appears because the Entrust Administrator has changed your name in the Entrust database. Typically this is because you legally changed your name within the corporate database and the change is being reflected within Entrust.

Another reason the message appears might be that, for some reason, your name and your Entrust information has been moved to a different location in the corporate database. Typically a change such as this affects many people at the same time and you will find that other users are also getting the same message when they log on to the Client. If you have not changed your name, ask your Entrust Administrator for an explanation.

Importing a key certified by a CA with the same name as your CA

Problem

The following message appears when you attempt to import a *key* file into your address book.



Entrust Error #: -490

Error while importing key. You cannot import a certificate with the same Certification Authority name as your own.

Reason

This message appears because the address in the *key* file you attempted to import into your address book was certified by a Certification Authority that is different from yours but has the same CA name. This provides a safeguard to prevent people from masquerading as internal Client users.

Appendix A: Entrust/Client shortcuts

You can use the mouse to perform all Client functions. Alternatively, you can use the keyboard. This appendix describes the keys you need to navigate through the Client.

Tab key

Press and release the *Tab* key to move from text field to text field in a dialog. A blinking I-beam pointer appears in each field as you tab.

Shift key

Use the *Shift* key in conjunction with the *Tab* key to reverse the direction in which the I-beam jumps from text field to text field. If you press the *Tab* key too many times and miss the field you want, you can hold down the *Shift* key and press the *Tab* key to move to the correct field.

Enter key

Pressing the *enter* key in a dialog is equivalent to clicking the button that is outlined in bold. This is usually the *OK* or *Done* button.

Return key

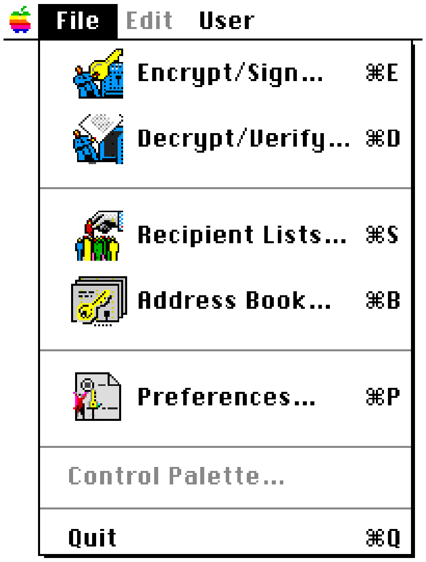
Pressing the *return* key in a dialog box is equivalent to clicking the button that is outlined in bold. This is usually the *OK* or *Done* button except in the *Select Entrust Recipients* dialog and the dialog for adding recipients to a group. In these dialogs, pressing the *return* key is equivalent to clicking the *Search* button.

Esc key

Pressing the *esc* key in a dialog is equivalent to clicking the *Cancel* button to leave a dialog without performing a function.

Keyboard shortcuts

As in other Macintosh applications, many commands that you choose from menus can also be invoked using keyboard shortcuts. A keyboard shortcut is a combination of keys that gives you the same result as choosing a command from a menu. A modifier key, usually the *Command* key, is pressed as you press another key. For example, Command-Q is the keyboard shortcut for quitting the Client application. Keyboard shortcuts are shown in a column beside the menu items.

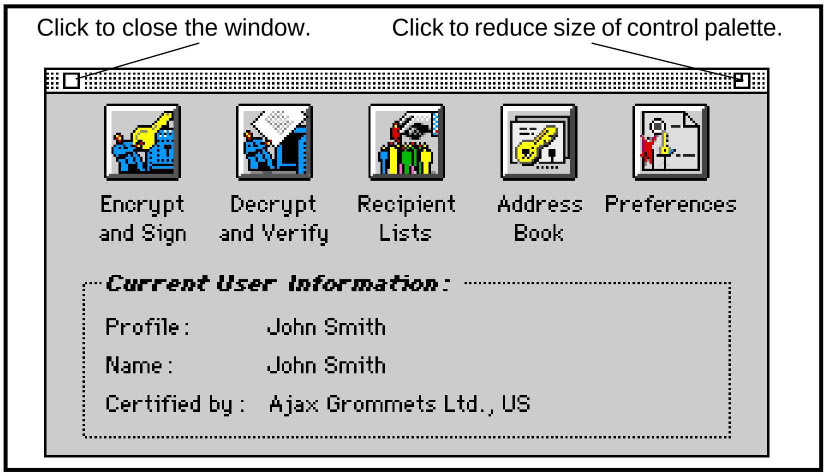


Control palette

The Entrust control palette (see Figure 8 on page 119) provides you with a set of icons that represent the main operations you can perform with the Client: Encrypt and Sign, Decrypt and Verify, Groups, Address Book, and Preferences. You can click the icon instead of accessing the operation from the *File* menu. The control palette appears on the desktop by default when you start the Client. However, you can choose to close it by clicking the top left corner of the palette. If you want to reopen it later, select *Control Palette...* from the *File* menu.

You can also change the size of the control palette by clicking the top right corner of the palette. When the palette appears in its full size and a user is currently logged on to the Client, the palette also displays the user's profile name, the name of the user, and the name of the Certification Authority.

Figure 8 Entrust control palette (full size)



Click to close the window.

Click to reduce size of control palette.

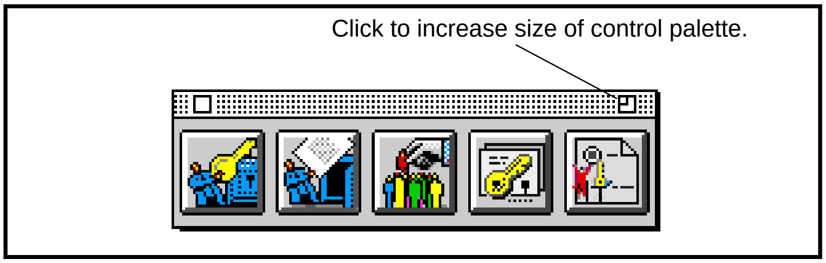
Current User Information:

Profile: John Smith

Name: John Smith

Certified by: Ajax Grommets Ltd., US

Figure 9 Entrust control palette (reduced size)



Click to increase size of control palette.

Appendix B: Entrust/Client user files

Client_username

This file contains your Client profile.

This profile contains your personal information which is required by the Client. This critical information is encrypted to ensure security. For increased security, you can store your Client profile permanently on a floppy diskette. Whenever you need to use the Client, you can access your profile via the floppy diskette.

This file is platform-independent, which means you can transfer this file to any computer in your organization running the Client and use it to log on to the Client. You may, however, need to rename your profile when your transfer it to another computer. For more information, refer to "Using Entrust/Client on different computers" on page 102.

ATTENTION

Do not delete or alter this file in any way. If you do, you will need to ask your Administrator to help you recover your profile.

Client_username.key

This file contains your personal Client address. By default, the filename comprises your Client username followed by *.key* (for example, *John Smith.key*).

If you want a person who uses the Client outside your organization to encrypt a file for you or to verify a file signed by you, give that person a copy of this file. When that external Client user encrypts a file for you, this file will provide the necessary information that will ensure you will be able to decrypt the file. See "Exchanging protected files with Entrust users in different domains" on page 71.

Client_username.erl

This file contains all your recipient lists, including any links to shared recipient lists you may have imported. By default, the filename is the same as your username. A *.erl* filename extension (for example, *johnsmit.erl*) is automatically added to the filename of the recipient lists file.

An Entrust/Client recipient list is a set of encryption and signing options, and a set of recipients that you select and store under a *recipient list* name. Instead of having to specify each recipient and option every time you want to encrypt a file, you can specify the name of a recipient list.

Refer to “Using saved lists of recipients” on page 80 for more information.

filename.srl

This file contain a single recipient list that has been designated as a shared recipient list. It is created by exporting a single recipient list. You can choose any filename when you export this file but the filename automatically receives a *.srl* filename extension (for example, *ourgroup.srl*). Refer to “Sharing recipient lists” on page 87 for more information.

Client_username.pab

This file contains your address book. By default, the filename comprises your Client username followed by a *.pab* filename extension (for example, *John Smith.pab*).

The address book contains addresses of people who use the Client outside your domain. These addresses allow you to encrypt files for these people so that they will be able to decrypt them.

For more information, refer to “Exchanging protected files with Entrust users in different domains” on page 71.

Entrust Prefs

This file contains important information required by the Client software. It is important not to modify the contents of this file, and not to move or delete the file. When you install the Client, a copy of this file is stored in your *Preferences* folder within your *System Folder.*

Appendix C: Entrust password security

Password security is a major concern for computer users. Exhaustive password searching attacks and dictionary attacks (two common methods for cracking passwords) represent serious threats to computer security. When you consider that an HP700 UNIX workstation can perform an exhaustive search of all possible combinations of six-letter (lower case) UNIX passwords in only 17 hours, it appears relatively easy for intruders to break into your system.

We understand your concerns. Passwords represent a critical link in the security chain. As a result, Entrust takes important steps to protect all passwords from even the most highly sophisticated schemes for attacking passwords.

When a user chooses a password, Entrust enforces the following rules to ensure that the password is secure:

- The password must contain a minimum of eight characters.
- The password must contain at least one upper case letter.
- The password must contain at least one lower case letter.
- The password must not contain many occurrences of the same character.

  The maximum number of occurrences of the same character allowed in your password is half the length of your password. For example, *mGmdmm&m* is not valid even though it contains eight characters. It is not valid because it contains five occurrences of the character *m* which is more than half the length of the password. The password *mGmtdm&m* is valid because it contains eight characters and it only contains four occurrences of the character *m* which is exactly half the length of the password.
- The password must not be the same as your Client username.

- The password must not contain a lengthy substring of your Client username.

  The maximum length of an allowable username substring is equal to half the length of your password. For example, if a username is *johnsmit*, the password *johnsM*4* is not valid even though it contains eight characters. It is not valid because it contains a five-character substring which can be found in the username, and five is more than half the length of the password. The password *johcmM*4* is valid because it contains eight characters and because it contains only a three-character substring which is less than half the length of the password.

Simply increasing the length of a password makes it less susceptible to attack. For example, increasing the password length from six to eight letters (lower case) changes the time to do an exhaustive search on UNIX passwords from 17 hours to 16 months. Moreover, when digits are introduced into eight-character passwords, the time required to do an exhaustive search on UNIX passwords increases to almost 18 years!

Once a user selects a password, Entrust applies a hash function to the password. Hash functions are often referred to as one-way hash functions, meaning that it is extremely difficult to determine the input to the one-way function if you have only the result of applying the function (that is, the function cannot be reversed). The result of the initial application of the hash function is then run through the hash function again, then again and again—in fact, the hash function is applied 100 times in succession.

Furthermore, prior to hashing, a unique quantity called a salt is appended to each user's password in a unique way. Using a unique salt for each password slows down password searches by attackers. With unique salts, an attacker must perform separate calculations for each password that is attacked. If the salts were not unique, an attacker could create a database of hashed passwords once (assuming the attacker knows the hash function), and then use this database to discover each password.

In addition, the complex calculations required to check a Client password take 50 times longer than the calculations required to check a UNIX password. That means that an attacker using an exhaustive search strategy would take approximately 65 years to search eight-letter (lower case) Client passwords versus only 16 months for equivalent UNIX passwords.

Entrust takes the result of iterating the original password through the hash function 100 times and uses that result as a key to encrypt a known value. The result of the encryption is referred to as the “password check value.” Only the password check value is stored in the user's Client profile. The original password is never stored by Entrust, making it impossible for someone to discover your password using a low-level disk utility program.

Later, when the user enters the original password while logging on to Entrust, the application reapplies the calculations listed above. The resulting check value is then compared against the stored password check value. If the two check values match, the user is allowed to log on to Entrust. Otherwise, the attempted log-on is rejected.

A more sophisticated attack than trying all combinations of characters is to guess dictionary words as passwords (known as a dictionary attack). While Entrust takes important steps to thwart dictionary attacks, users can further protect their passwords by taking the following precautions:

- using a mixture of letters (upper and lower case), digits, and special characters (for example, @ and !)
- creating passwords longer than eight characters
- avoiding words found in dictionaries

Note: Calculations used in this appendix are done assuming computing capabilities equivalent to those in an HP700 UNIX workstation.

Appendix D: Entrust specifications

Cryptographic algorithms and standards

Encryption

- U.S. Data Encryption Standard (DES) in accordance with U.S. FIPS PUB 46-2 and ANSI X3.92
- Northern Telecom CAST algorithm
- DES and CAST encryption using CBC mode of operation in accordance with U.S. FIPS PUB 81, ANSI X3.106 and ISO/IEC 10116

Digital signatures

- RSA digital signature in accordance with RSA Data Security Inc. Public Key Cryptographic Standards (PKCS) specification PKCS#1

Hash functions

- MD2 Message-Digest algorithm in accordance with Internet RFC 1319
- MD5 Message-Digest algorithm in accordance with Internet RFC 1321

Key management

- RSA key transfer in accordance with Internet RFC 1421 and 1423 (PEM)

Integrity

- Message Authentication Code (MAC) in accordance with U.S. FIPS PUB 113 and ANSI X9.9

Pseudo-random number generation

- As given in ANSI X9.17

Data formats and protocols

Certificate formats

- Public-key certificates in accordance with ITU-T Rec. X.509 (1993), ISO/IEC 9594-8 (1995), and Draft Amendment 1 to ISO/IEC 9594-8 (1995)
- Certificate revocation lists in accordance with ITU-T Rec. X.509 (1993), ISO/IEC 9594-8 (1995), and Draft Amendment 1 to ISO/IEC 9594-8 (1995)
- RSA algorithm identifiers and public key formats in accordance with Internet RFC 1422 and 1423 (PEM)

File envelope format

- Based on Internet RFC 1421 (PEM)

Directory protocols

- Directory Access Protocol (DAP) and Directory System Protocol (DSP) in accordance with ITU-T Rec. X.500 and ISO/IEC 9594
- Lightweight Directory Access Protocol (LDAP) in accordance with Internet RFC 1777
- Entrust/Server is based on the University of Michigan's LDAP server, ldapd

Client management protocol

- Northern Telecom Security Exchange Protocol (SEP), built using Generic Upper Layers Security (GULS) standards based on ITU-T Recs. 830, 831, 832 and ISO/IEC 11586-1, 11586-2, 11586-3

Software interfaces

Application program interfaces (APIs)

- Online mode API in accordance with Internet Generic Security Services (GSS)-API specification in Internet RFCs 1508 and 1509
- Online mode GSS-API mechanism using Internet Simple Public Key Mechanism (SPKM) (proposed Internet Standard)

- Store-and-forward API in accordance with Entrust/Toolkit API specification

Government endorsement

- Cryptographic module validation to level 1 under U.S. FIPS PUB 140-1
- Canadian Government Cryptographic Endorsement and Assessment Program (CEAP) (evaluation in progress)

List of terms

address book

An address book contains the Entrust addresses of people in other organizations for whom you plan to encrypt and sign files.

Administrator

See Entrust Administrator.

authorization code

A code (for example, 7NGP-Q3I6-HAWG), obtained from your Entrust Administrator, which is required along with a reference number to create a new Entrust/Client username or to recover an existing username. The authorization code can only be used once and then it is no longer valid.

Certification Authority

Typically, in each organization there are people who are responsible for setting policies regarding the protection of sensitive and valuable data. Within the context of Entrust, these people are referred to collectively as the Certification Authority (CA).

The people who are responsible for implementing these security policies are called Security Officers and Entrust Administrators. These people act on behalf of the CA.

Client

See Entrust/Client.

decrypt

To decrypt a protected file is to restore it to its original, unprotected state.

defaults

Various operations, options, and entry fields have default values in the Client. These values can be changed in the preferences dialog.

destination folder

In the Client, the designated folder that receives protected or unprotected files, depending on the operation(s) being performed.

digital signature

The result of making a mathematical summary (known as a *hash*) of data and signing the hash with a private key known only to a specific authorized user. The signature can be verified by any other user who has the corresponding verification public key. A digital signature provides a guarantee to a recipient that a file came from the person who sent it, and that it was not altered since it was signed.

domain

See Entrust domain.

drag and drop

The process of selecting one or more files on the desktop in the Finder using the mouse, and dragging them to Entrust. Refer to “Dragging and dropping files” on page 26 for information about dragging and dropping files.

encrypt

To encrypt a file is to render the file completely unreadable. That means no one, including you, can read the file until it is decrypted. Only you and the authorized recipients can decrypt the file. You have full control in determining authorized recipients.

Entrust address

An Entrust address provides the necessary information to ensure that files encrypted and signed by someone using Entrust in one domain can be decrypted and verified by someone using Entrust in other domains.

An Entrust address is stored in a *key* file and all users can export their own *key* file. The filename comprises your Client username with a *key* filename suffix (for example, *John Smith.key*). For information about exporting your Entrust address, refer to “Exporting your personal Entrust address” on page 78.

Entrust domain

An Entrust domain is a group of Entrust users who have all been certified by the same Certification Authority under one software license. Typically these users have something in common (for example, they all work in the same company or they work on the same project). It is possible to have several Entrust domains in the same company. What differentiates one domain from another is the Certification Authority that certifies users in the domain.

Entrust Administrator

This is a person within your Entrust domain who has the responsibility of maintaining all aspects of the Client. This job includes enabling and recovering Client users. The Administrator should be trusted by everyone in the Entrust domain.

Entrust/Client

A software application that allows people to encrypt files, decrypt files, digitally sign files, and verify digital signatures on files.

Entrust/Manager

A database that manages cryptographic keys for Entrust users.

Entrust/Client profile

Your profile is a file that contains critical information about you which is required by Entrust. This critical information is encrypted to ensure security. The filename of your profile is the same as your username (for example, *John Smith*).

Entrust recipients

People to whom you have given authorization to decrypt some of your files.

personal address book

See address book.

profile

See Entrust/Client profile.

recipient list

An Entrust/Client recipient list is a set of encryption and/or signing options, and/or a set of recipients that you select and store under a *recipient list* name. Instead of having to specify each recipient and/or option every time you want to encrypt a file, you can specify the name of a recipient list.

Refer to “Using saved lists of recipients” on page 80 for more information.

recipients

See Entrust recipients.

reference number

A number (for example, 91208050), obtained from your Entrust Administrator, which is used along with an authorization code to create a new Entrust/Client username or to recover lost data associated with an existing user.

secret

In this document, secret refers to information that should not be divulged to anyone. For example, passwords must remain secret.

validation string

A validation string is a string of alphanumeric characters (for example, 7CN4-YL5D-HP7V) that is automatically generated by the Client when you export your address. Each Entrust address has a unique validation string which is associated with the *key* file. Use the validation string to confirm that the address someone gives you in a *key* file has not been modified since it was created.

Index

Nortel Secure Networks

Entrust/Client

User Guide

for the Macintosh

This information is subject to change as Northern Telecom Limited reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances may warrant.

Publication number: 68008.08
Date: January 1996
Software release: 2
Printed in Canada

NORTEL